MAX-200M1 Series

IEEE 802.16e Simple Indoor CPE

User's Guide

Version 3.60
04/2007
Edition 1

ZyXEL

Copyright

Copyright © 2007 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- The device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2). End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Viewing Certifications

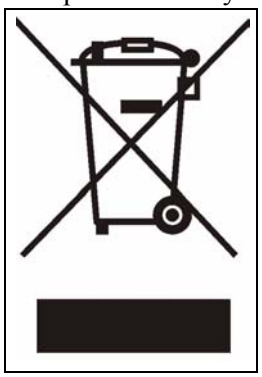
1. Go to http://www.zyxel.com.
2. Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- ONLY qualified service personnel should service or disassemble this device.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).

This product is recyclable. Dispose of it properly.



ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Customer Support

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE / FAX	WEB SITE / FTP SITE	REGULAR MAIL
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
COSTA RICA	soporte@zyxel.co.cr	+506-2017878	www.zyxel.co.cr	ZyXEL Costa Rica Plaza Roble Escazú Etapa El Patio, Tercer Piso San José, Costa Rica
	sales@zyxel.co.cr	+506-2015098	ftp.zyxel.co.cr	
CZECH REPUBLIC	info@cz.zyxel.com	+420-241-091-350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
	info@cz.zyxel.com	+420-241-091-359		
DENMARK	support@zyxel.dk	+45-39-55-07-00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 2860 Soeborg Denmark
	sales@zyxel.dk	+45-39-55-07-07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33-4-72-52-97-97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33-4-72-52-19-20		
GERMANY	support@zyxel.de	+49-2405-6909-69	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
HUNGARY	support@zyxel.hu	+36-1-3361649	www.zyxel.hu	ZyXEL Hungary 48, Zoldlomb Str. H-1025, Budapest Hungary
	info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN	http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave.,Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
	sales@zyxel.kz	+7-3272-590-689		
NORTH AMERICA	support@zyxel.com	1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	

METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE / FAX	WEB SITE / FTP SITE	REGULAR MAIL
NORWAY	support@zyxel.no sales@zyxel.no	+47-22-80-61-80 +47-22-80-61-81	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
POLAND	info@pl.zyxel.com	+48 (22) 333 8250 +48 (22) 333 8251	www.pl.zyxel.com	ZyXEL Communications ul. Okrzei 1A 03-715 Warszawa Poland
RUSSIA	http://zyxel.ru/support sales@zyxel.ru	+7-095-542-89-29 +7-095-542-89-25	www.zyxel.ru	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
SPAIN	support@zyxel.es sales@zyxel.es	+34-902-195-420 +34-913-005-345	www.zyxel.es	ZyXEL Communications Arte, 21 5ª planta 28033 Madrid Spain
SWEDEN	support@zyxel.se sales@zyxel.se	+46-31-744-7700 +46-31-744-7701	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
UKRAINE	support@ua.zyxel.com sales@ua.zyxel.com	+380-44-247-69-78 +380-44-494-49-32	www.ua.zyxel.com	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
UNITED KINGDOM	support@zyxel.co.uk sales@zyxel.co.uk	+44-1344 303044 08707 555779 (UK only) +44-1344 303034	www.zyxel.co.uk ftp.zyxel.co.uk	ZyXEL Communications UK Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)

+" is the (prefix) number you enter to make an international telephone call.

Table of Contents

Copyright **3**

Certifications **4**

Safety Warnings **6**

ZyXEL Limited Warranty **8**

Customer Support **9**

Table of Contents **11**

List of Figures **19**

List of Tables **23**

Preface **27**

Chapter 1
Getting Started **29**

1.1 About Your ZyXEL Device 29
1.1.1 Wireless Internet Access 29
1.1.2 Make Calls via Internet Telephony Service Provider 30
1.2 ZyXEL Device Hardware 31
1.2.1 LEDs 31
1.2.2 Antenna 32

Chapter 2
Introducing the Web Configurator **33**

2.1 Web Configurator Overview 33
2.1.1 Accessing the Web Configurator 33
2.1.2 The RESET Button 35
2.1.2.1 Using The Reset Button 35
2.2 Web Configurator Main Screen 36
2.2.1 Title Bar 36
2.2.2 Navigation Panel 37
2.2.3 Main Window 39
2.2.4 Status Bar 39

Chapter 3
Tutorial 41

3.1 Connect to the Internet 41
3.1.1 Configure Internet Access Settings 41
3.1.2 Configure WiMAX Settings 42
3.2 Make a Telephone Call Over the Internet 43
3.2.1 Configure Your SIP Account 44
3.2.2 Configure a Phone 45
3.2.3 Set Up Speed Dialing and Make a Call 46

Chapter 4
Internet Setup Wizard 49

4.1 Wizard Setup Overview 49
4.2 Internet Connection Wizard Setup 49

Chapter 5
VoIP Wizard 55

5.1 Introduction 55
5.2 VOIP Wizard Setup 55

Chapter 6
Status Screens 59

6.1 Status Screen 59
6.2 Site Information 63
6.3 Profile 64
6.4 Any IP Table Window 65
6.5 Packet Statistics 66
6.6 DHCP Table Screen 67
6.7 VoIP Statistics Window 68

Chapter 7
WAN Setup 71

7.1 WAN Overview 71
7.2 WiMAX 71
7.2.1 Authentication 72
7.3 Internet Access Setup 72
7.4 Frequency Settings 74
7.4.1 Frequency Ranges 75
7.4.2 Configuring Frequency Settings 75
7.4.2.1 Using the WiMAX Frequency Screen: Example 77
7.5 Configuring Advanced WAN Settings 78
7.6 Configuring Traffic Redirect Settings 80

Chapter 8
LAN 83

8.1 LAN Overview 83
8.1.1 IP Address and Subnet Mask 83
8.1.2 DHCP Setup 84
8.1.3 LAN TCP/IP 84
8.1.4 DNS Server Address 84
8.1.5 RIP Setup 85
8.1.6 Multicast 85
8.1.7 Any IP 86
8.2 LAN Screens 88
8.2.1 LAN IP Screen 88
8.2.2 LAN DHCP Setup Screen 88
8.2.3 LAN Static DHCP Screen 89
8.2.4 LAN Client List Screen 90
8.2.5 LAN IP Alias Screen 91
8.2.6 LAN Advanced Screen 93

Chapter 9
NAT 97

9.1 NAT Overview 97
9.1.1 Port Forwarding: Services and Port Numbers 97
9.1.2 Trigger Port Forwarding 98
9.1.2.1 Trigger Port Forwarding Example 98
9.1.2.2 Two Points To Remember About Trigger Ports 99
9.1.3 SIP ALG 99
9.2 NAT Screens 99
9.2.1 NAT General Screen 99
9.2.2 NAT Port Forwarding Screen 100
9.2.3 NAT Port Forwarding Edit Screen 102
9.2.4 NAT Trigger Port Screen 102
9.2.5 NAT ALG Screen 104

Chapter 10
SIP 105

10.1 SIP Overview 105
10.1.1 Introduction to VoIP 105
10.1.2 Introduction to SIP 105
10.1.3 SIP Identities 105
10.1.3.1 SIP Number 105
10.1.3.2 SIP Service Domain 106
10.1.4 SIP Call Progression 106
10.1.5 SIP Client Server 106

10.1.5.1 SIP User Agent 107
10.1.5.2 SIP Proxy Server 107
10.1.5.3 SIP Redirect Server 108
10.1.5.4 SIP Register Server 108
10.1.6 RTP 108
10.1.7 NAT and SIP 109
10.1.7.1 SIP ALG 109
10.1.7.2 Use NAT 109
10.1.7.3 STUN 109
10.1.7.4 Outbound Proxy 110
10.1.8 Voice Coding 110
10.1.9 PSTN Call Setup Signaling 111
10.1.10 MWI (Message Waiting Indication) 111
10.1.11 Custom Tones (IVR) 111
10.1.11.1 Recording Custom Tones 112
10.1.11.2 Listening to Custom Tones 112
10.1.11.3 Deleting Custom Tones 112
10.1.12 Quality of Service (QoS) 112
10.1.12.1 Type Of Service (ToS) 112
10.1.12.2 DiffServ 113
10.1.12.3 DSCP and Per-Hop Behavior 113
10.1.12.4 VLAN 113
10.2 SIP Screens 114
10.2.1 SIP Settings Screen 114
10.2.2 Advanced SIP Setup Screen 115
10.2.3 SIP QoS Screen 119

Chapter 11
Phone 121

11.1 Phone Overview 121
11.1.1 Voice Activity Detection/Silence Suppression/Comfort Noise 121
11.1.2 Echo Cancellation 121
11.1.3 Supplementary Phone Services Overview 121
11.1.3.1 The Flash Key 122
11.1.3.2 Europe Type Supplementary Phone Services 122
11.1.3.3 USA Type Supplementary Services 124
11.2 Phone Screens 125
11.2.1 Analog Phone Screen 125
11.2.2 Advanced Analog Phone Setup Screen 126
11.2.3 Common Phone Settings Screen 128
11.2.4 Phone Region Screen 128

Chapter 12
Firewall 131

12.1 Firewall Overview 131
12.1.1 Stateful Inspection Firewall. 131
12.1.2 About the ZyXEL Device Firewall 131
12.1.3 Guidelines For Enhancing Security With Your Firewall 132
12.1.4 The Firewall, NAT and Remote Management 132
12.1.4.1 LAN-to-WAN rules 132
12.1.4.2 WAN-to-LAN rules 133
12.2 Triangle Route 133
12.2.1 The "Triangle Route" Problem 134
12.2.2 Solving the "Triangle Route" Problem 134
12.3 Firewall Screens 135
12.3.1 General Firewall Screen 135
12.3.2 Firewall Services Screen 136

Chapter 13
Phone Book 139

13.1 Phone Book Overview 139
13.2 Phone Book Screens 139
13.2.1 Incoming Call Policy Screen 139
13.2.2 Speed Dial Screen 141

Chapter 14
Content Filter 145

14.1 Content Filtering Overview 145
14.2 Content Filtering Screens 145
14.2.1 Content Filter Screen 145
14.2.2 Content Filter Schedule Screen 147

Chapter 15
Static Route 149

15.1 Static Route Overview 149
15.2 Static Route Screens 149
15.2.1 IP Static Route Screen 149
15.2.2 IP Static Route Edit Screen 150

Chapter 16
Remote MGMT 153

16.1 Remote Management Overview 153
16.1.1 Remote Management Limitations 153
16.1.2 Remote Management and NAT 154
16.1.3 System Timeout 154

16.2 Remote Management Screens 154
16.2.1 WWW Screen 154
16.2.2 Telnet Screen 155
16.2.3 FTP Screen 155
16.3 SNMP 156
16.3.1 Supported MIBs 157
16.3.2 SNMP Traps 158
16.3.3 Configuring SNMP 158
16.3.4 DNS Screen 160
16.3.5 Security Screen 160

Chapter 17
UPnP 163

17.1 Introducing Universal Plug and Play 163
17.1.1 How do I know if I'm using UPnP? 163
17.1.2 NAT Traversal 163
17.1.3 Cautions with UPnP 163
17.1.4 UPnP and ZyXEL 164
17.2 UPnP Examples 164
17.2.1 Installing UPnP in Windows Example 164
17.2.1.1 Installing UPnP in Windows Me 164
17.2.1.2 Installing UPnP in Windows XP 166
17.2.2 Using UPnP in Windows XP Example 167
17.2.2.1 Auto-discover Your UPnP-enabled Network Device 167
17.2.2.2 Web Configurator Easy Access 171
17.3 UPnP Screen 174

Chapter 18
Logs 177

18.1 Logs Overview 177
18.1.1 Alerts 177
18.1.2 Syslog Logs 177
18.2 Logs Screens 179
18.2.1 Log Viewer Screen 179
18.2.2 Log Settings Screen 179
18.3 Log Message Descriptions 182

Chapter 19
Tools 191

19.1 Tools Overview 191
19.1.1 ZyXEL Firmware 191
19.2 Tools Screens 191
19.2.1 Firmware Screen 191

19.2.2 Firmware Upload Screens 192
19.2.3 Configuration Screen 193
19.2.4 Restore Configuration Screens 194
19.2.5 Restart Screen 195

Chapter 20
System 197

20.1 System Features Overview 197
20.1.1 System Name 197
20.1.2 Domain Name 197
20.1.3 DNS Server Address Assignment 197
20.1.4 Dynamic DNS 198
20.1.5 Pre-defined NTP Time Servers List 198
20.1.6 Resetting the Time 199
20.2 System Screens 199
20.2.1 General System Screen 199
20.2.2 Dynamic DNS Screen 200
20.2.3 Time Setting Screen 202

Chapter 21
Troubleshooting 205

21.1 Problems Starting Up the ZyXEL Device 205
21.2 Problems with the LAN 205
21.3 Problems with the WAN 206
21.4 Problems with the Link Quality 206
21.5 Problems Accessing the ZyXEL Device 207
21.5.1 Pop-up Windows, JavaScripts and Java Permissions 207
21.5.1.1 Internet Explorer Pop-up Blockers 208
21.5.1.2 JavaScripts 211
21.5.1.3 Java Permissions 212
21.6 Telephone Problems 213
21.7 Problems With Multiple SIP Accounts 214

Appendix A
Product Specifications 215

Appendix B
WiMAX Security 219

User Authentication and Data Encryption 219
RADIUS 220
Security Association 221
Authentication 222

Appendix C
Setting up Your Computer's IP Address 223

Windows 95/98/Me 223
Windows 2000/NT/XP 226
Macintosh OS X 231
Linux 233

Appendix D
IP Addresses and Subnetting 237

Introduction to IP Addresses 237
Structure 237
Subnet Masks 238
Notation 239
Subnetting 240
Example: Four Subnets 241
Example: Eight Subnets 242
Subnet Planning 243
Configuring IP Addresses 244

Appendix E
SIP Passthrough 247

Enabling/Disabling the SIP ALG 247
Signaling Session Timeout 247
Audio Session Timeout 247

Appendix F
Services 249

Index 253

List of Figures

Figure 1 Mobile Station and Base Station 30
Figure 2 ZyXEL Device's VoIP Features 30
Figure 3 The ZyXEL Device 31
Figure 4 Password Screen 34
Figure 5 Change Password Screen 34
Figure 6 Replace Certificate Screen 34
Figure 7 Wizard or Advanced Screen 35
Figure 8 Main Screen 36
Figure 9 Tutorial: Navigation Panel 41
Figure 10 Tutorial: Internet Access Settings 42
Figure 11 Tutorial: WiMAX Frequency Setup 43
Figure 12 Tutorial: SIP Account Setup 44
Figure 13 Tutorial: the Analog Phone Screen 45
Figure 14 Tutorial: the Speed Dial Screen 46
Figure 15 Tutorial: New Speed Dial Rule 47
Figure 16 Select a Mode 49
Figure 17 Connection Wizard: Introduction 50
Figure 18 The Connection Wizard: System Information 50
Figure 19 The Connection Wizard: Internet Configuration 1 51
Figure 20 The Connection Wizard: ISP Username and Password 51
Figure 21 The Connection Wizard: Your IP Address 52
Figure 22 The Connection Wizard: WAN IP Address Assignment 52
Figure 23 The Connection Wizard: WAN MAC Address 53
Figure 24 The Connection Wizard: Congratulations 53
Figure 25 Select a Mode 55
Figure 26 VOIP Wizard: Configuration 56
Figure 27 VoIP Wizard: SIP Registration Test 57
Figure 28 VoIP Wizard: Fail 57
Figure 29 VOIP Wizard: Finish 57
Figure 30 Status Screen 59
Figure 31 The Site Information Screen 64
Figure 32 The WiMAX Profile Screen 65
Figure 33 Any IP Table 66
Figure 34 Packet Statistics 67
Figure 35 DHCP Table 68
Figure 36 VoIP Statistics 69
Figure 37 WiMax: Mobile Station 71
Figure 38 WiMAX: Multiple Mobile Stations 72

Figure 39 Using an AAA Server 72
Figure 40 Network > WAN > Internet Connection 73
Figure 41 Frequency Ranges 75
Figure 42 Network > WAN >WiMAX Frequency 77
Figure 43 Completing the WiMAX Frequency Screen 78
Figure 44 Network > WAN > Advanced 79
Figure 45 Network > WAN > Traffic Redirect 80
Figure 46 Any IP Example 87
Figure 47 Network > LAN > IP 88
Figure 48 Network > LAN > DHCP Setup 89
Figure 49 Network > LAN > Static DHCP 90
Figure 50 Network > LAN > Client List 91
Figure 51 Network > LAN > IP Alias 92
Figure 52 Network > LAN > Advanced 94
Figure 53 Multiple Servers Behind NAT Example 98
Figure 54 Trigger Port Forwarding Process: Example 98
Figure 55 Network > NAT > General 100
Figure 56 Network > NAT > Port Forwarding 101
Figure 57 Network > NAT > Port Forwarding > Edit 102
Figure 58 Network > NAT > Trigger Port 103
Figure 59 Network > NAT > ALG 104
Figure 60 SIP User Agent 107
Figure 61 SIP Proxy Server 107
Figure 62 SIP Redirect Server 108
Figure 63 STUN 110
Figure 64 DiffServ: Differentiated Service Field 113
Figure 65 VoIP > SIP > SIP Settings 114
Figure 66 VoIP > SIP > SIP Settings > Advanced 116
Figure 67 VoIP > SIP > QoS 120
Figure 68 VoIP > Phone > Analog Phone 125
Figure 69 VoIP > Phone > Analog Phone > Advanced 127
Figure 70 VoIP > Phone > Common 128
Figure 71 VoIP > Phone > Region 129
Figure 72 Firewall Rule Directions 132
Figure 73 Ideal Firewall Setup 133
Figure 74 "Triangle Route" Problem 134
Figure 75 IP Alias 135
Figure 76 Security > Firewall > General 136
Figure 77 Security > Firewall > Services 137
Figure 78 VoIP > Phone Book > Incoming Call Policy 140
Figure 79 VoIP > Phone Book > Speed Dial 142
Figure 80 Security > Content Filter > Filter 146
Figure 81 Security > Content Filter > Schedule 147

Figure 82 Example of Static Routing Topology 149
Figure 83 Management > Static Route > IP Static Route 150
Figure 84 Management > Static Route > IP Static Route > Edit 151
Figure 85 Management > Remote MGMT > WWW 154
Figure 86 Management > Remote MGMT > Telnet 155
Figure 87 Management > Remote MGMT > FTP 156
Figure 88 SNMP Management Model 157
Figure 89 Management > Remote MGMT > SNMP 159
Figure 90 Management > Remote MGMT > DNS 160
Figure 91 Management > Remote MGMT > Security 161
Figure 92 Add/Remove Programs: Windows Setup: Communication 165
Figure 93 Add/Remove Programs: Windows Setup: Communication Components 165
Figure 94 Network Connections 166
Figure 95 Windows Optional Networking Components Wizard 166
Figure 96 Networking Services 167
Figure 97 Network Connections 168
Figure 98 Internet Connection Properties 169
Figure 99 Internet Connection Properties: Advanced Settings 170
Figure 100 Internet Connection Properties: Advanced Settings: Add 170
Figure 101 System Tray Icon 171
Figure 102 Internet Connection Status 171
Figure 103 Network Connections 172
Figure 104 Network Connections: My Network Places 173
Figure 105 Network Connections: My Network Places: Properties: Example 174
Figure 106 Management > UPnP 175
Figure 107 Maintenance > Logs > View Log 179
Figure 108 Maintenance > Logs > Log Settings 180
Figure 109 Maintenance > Tools > Firmware 192
Figure 110 Firmware Upload In Process 192
Figure 111 Network Temporarily Disconnected 193
Figure 112 Firmware Upload Error 193
Figure 113 Maintenance > Tools > Configuration 194
Figure 114 Configuration Upload Successful 195
Figure 115 Network Temporarily Disconnected 195
Figure 116 Configuration Upload Error 195
Figure 117 Maintenance > Tools > Restart 196
Figure 118 Maintenance > Tools > Restart > In Progress 196
Figure 119 Maintenance > System > General 200
Figure 120 Maintenance > System > Dynamic DNS 201
Figure 121 Maintenance > System > Time Setting 203
Figure 122 Pop-up Blocker 208
Figure 123 Internet Options 209
Figure 124 Internet Options 210

Figure 125 Pop-up Blocker Settings 210
Figure 126 Internet Options 211
Figure 127 Security Settings - Java Scripting 212
Figure 128 Security Settings - Java 212
Figure 129 Java (Sun) 213
Figure 130 WIndows 95/98/Me: Network: Configuration 224
Figure 131 Windows 95/98/Me: TCP/IP Properties: IP Address 225
Figure 132 Windows 95/98/Me: TCP/IP Properties: DNS Configuration 226
Figure 133 Windows XP: Start Menu 227
Figure 134 Windows XP: Control Panel 227
Figure 135 Windows XP: Control Panel: Network Connections: Properties 228
Figure 136 Windows XP: Local Area Connection Properties 228
Figure 137 Windows XP: Internet Protocol (TCP/IP) Properties 229
Figure 138 Windows XP: Advanced TCP/IP Properties 230
Figure 139 Windows XP: Internet Protocol (TCP/IP) Properties 231
Figure 140 Macintosh OS X: Apple Menu 232
Figure 141 Macintosh OS X: Network 232
Figure 142 Red Hat 9.0: KDE: Network Configuration: Devices 233
Figure 143 Red Hat 9.0: KDE: Ethernet Device: General 234
Figure 144 Red Hat 9.0: KDE: Network Configuration: DNS 234
Figure 145 Red Hat 9.0: KDE: Network Configuration: Activate 235
Figure 146 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 235
Figure 147 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 236
Figure 148 Red Hat 9.0: DNS Settings in resolv.conf 236
Figure 149 Red Hat 9.0: Restart Ethernet Card 236
Figure 150 Red Hat 9.0: Checking TCP/IP Properties 236
Figure 151 Network Number and Host ID 238
Figure 152 Subnetting Example: Before Subnetting 240
Figure 153 Subnetting Example: After Subnetting 241

List of Tables

Table 1 Models Covered 29
Table 2 The ZyXEL Device 31
Table 3 Web Configurator Icons in the Title Bar 37
Table 4 Navigation Panel Summary 37
Table 5 VOIP Wizard Configuration 56
Table 6 Status Screen 60
Table 7 The Site Information Screen 64
Table 8 The WiMAX Profile Screen 65
Table 9 Any IP Table 66
Table 10 Packet Statistics 67
Table 11 DHCP Table 68
Table 12 VoIP Statistics 69
Table 13 Network > WAN > Internet Connection 73
Table 14 Radio Frequency Conversion 75
Table 15 DL Frequency Example Settings 76
Table 16 Network > WAN > WiMAX Frequency 77
Table 17 Example Supported Frequencies (GHz) 77
Table 18 Network > WAN > Advanced 79
Table 19 Network > WAN > Traffic Redirect 80
Table 20 Network > LAN > IP 88
Table 21 Network > LAN > DHCP Setup 89
Table 22 Network > LAN > Static DHCP 90
Table 23 Network > LAN > Client List 91
Table 24 Network > LAN > IP Alias 92
Table 25 Network > LAN > Advanced 94
Table 26 Network > NAT > General 100
Table 27 Network > NAT > Port Forwarding 101
Table 28 Network > NAT > Port Forwarding > Edit 102
Table 29 Network > NAT > Trigger Port 103
Table 30 Network > NAT > ALG 104
Table 31 SIP Call Progression 106
Table 32 Custom Tones Details 111
Table 33 VoIP > SIP > SIP Settings 114
Table 34 VoIP > SIP > SIP Settings > Advanced 117
Table 35 VoIP > SIP > QoS 120
Table 36 European Type Flash Key Commands 122
Table 37 USA Type Flash Key Commands 124
Table 38 VoIP > Phone > Analog Phone 125

Table 39 VoIP > Phone > Analog Phone > Advanced 127
Table 40 VoIP > Phone > Common 128
Table 41 VoIP > Phone > Region 129
Table 42 Security > Firewall > General 136
Table 43 Security > Firewall > Services 137
Table 44 VoIP > Phone Book > Incoming Call Policy 140
Table 45 VoIP > Phone Book > Speed Dial 142
Table 46 Security > Content Filter > Filter 146
Table 47 Security > Content Filter > Schedule 147
Table 48 Management > Static Route > IP Static Route 150
Table 49 Management > Static Route > IP Static Route > Edit 151
Table 50 Management > Remote MGMT > WWW 154
Table 51 Management > Remote MGMT > Telnet 155
Table 52 Management > Remote MGMT > FTP 156
Table 53 SNMP Traps 158
Table 54 Remote Management: SNMP 159
Table 55 Management > Remote MGMT > DNS 160
Table 56 Management > Remote MGMT > Security 161
Table 57 Management > UPnP 175
Table 58 Syslog Logs 178
Table 59 RFC-2408 ISAKMP Payload Types 178
Table 60 Maintenance > Logs > View Log 179
Table 61 Maintenance > Logs > Log Settings 180
Table 62 System Error Logs 182
Table 63 System Maintenance Logs 182
Table 64 Access Control Logs 183
Table 65 TCP Reset Logs 183
Table 66 Packet Filter Logs 184
Table 67 ICMP Logs 184
Table 68 CDR Logs 185
Table 69 PPP Logs 185
Table 70 UPnP Logs 185
Table 71 Content Filtering Logs 186
Table 72 Attack Logs 186
Table 73 Remote Management Logs 187
Table 74 ICMP Notes 188
Table 75 SIP Logs 189
Table 76 RTP Logs 189
Table 77 FSM Logs: Caller Side 190
Table 78 FSM Logs: Callee Side 190
Table 79 Lifeline Logs 190
Table 80 Maintenance > Tools > Firmware 192
Table 81 Maintenance > Tools > Configuration 194

Table 82 Pre-defined NTP Time Servers 198
Table 83 Maintenance > System > General 200
Table 84 Maintenance > System > Dynamic DNS 201
Table 85 Maintenance > System > Time Setting 203
Table 86 Troubleshooting Starting Up Your Device 205
Table 87 Troubleshooting the LAN 205
Table 88 Troubleshooting the WAN 206
Table 89 Troubleshooting Link Quality 206
Table 90 Troubleshooting Accessing Your Device 207
Table 91 Troubleshooting Telephone 213
Table 92 Product Specifications 215
Table 93 Physical Features 216
Table 94 Non-Physical Features 216
Table 95 IP Address Network Number and Host ID Example 238
Table 96 Subnet Masks 239
Table 97 Maximum Host Numbers 239
Table 98 Alternative Subnet Mask Notation 239
Table 99 Subnet 1 241
Table 100 Subnet 2 242
Table 101 Subnet 3 242
Table 102 Subnet 4 242
Table 103 Eight Subnets 242
Table 104 24-bit Network Number Subnet Planning 243
Table 105 16-bit Network Number Subnet Planning 243
Table 106 Examples of Services 249

Preface

Congratulations on your purchase of the ZyXEL MAX-200M1 Series IEEE 802.16e Simple Indoor CPE. Your ZyXEL Device allows you to access WiMAX wireless networks and make Voice over Internet (VoIP) phone calls.

Your ZyXEL Device is easy to install and configure.

About This User's Guide

This manual is designed to guide you through the configuration of your ZyXEL Device for its various applications.

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains hardware installation/connection information.

- ZyXEL Web Site

  Please go to http://www.zyxel.com for product news, firmware, updated documents, and other support materials.

User Guide Feedback

Help us help you. E-mail all User's Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one predefined choice.
- Mouse action sequences are denoted by right angle brackets (>). For example, "**Start** > **Settings** > **Control Panel** > **System**" means click the **Start** button, move the mouse over **Settings**, move the mouse over or click on **Control Panel**, and then click on **System**.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".
- The ZyXEL MAX-200M1 Series IEEE 802.16e Simple Indoor CPE may be referred to as "the ZyXEL Device" or "the device" in this User's Guide.

Graphics Icons Key

ZyXEL Device	Computer	Notebook Computer
Wireless Signal	Wireless Base Station	Internet Cloud
Router	Server	

CHAPTER 1
Getting Started

This chapter introduces the main features and applications of the ZyXEL Device.

1.1 About Your ZyXEL Device

The ZyXEL Device is a WiMAX wireless network adapter. It allows you to access the Internet by connecting to a WiMAX wireless network.

You can use a traditional analog telephone to make Internet calls using the ZyXEL Device's Voice over IP (VoIP) communication capabilities.

You can configure firewall and content filtering for secure Internet access, as well as a host of other features.

The web browser-based Graphical User Interface (GUI), also known as the web configurator, provides easy management.

See Appendix A on page 215 for a complete list of features for your model.

At the time of writing, this User's Guide covers the following models:

Table 1 Models Covered

MAX-200M1
MAX-210M1
MAX-230M1

This User's Guide uses screens and example settings from the MAX-200M1 model.

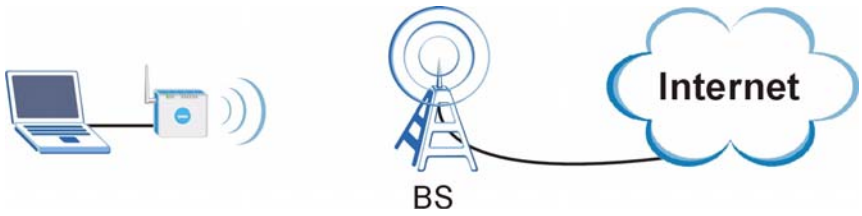
1.1.1 Wireless Internet Access

Connect your computer or network to the ZyXEL Device for wireless Internet access. See the Quick Start Guide for instructions on hardware connection.

In a wireless metropolitan area network (MAN), the ZyXEL Device connects to a base station (BS) for Internet access.

The following diagram shows a notebook computer equipped with the ZyXEL Device connecting to the Internet through a base station (marked **BS**).

Figure 1 Mobile Station and Base Station



You can also configure firewall and content filtering on the ZyXEL Device for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

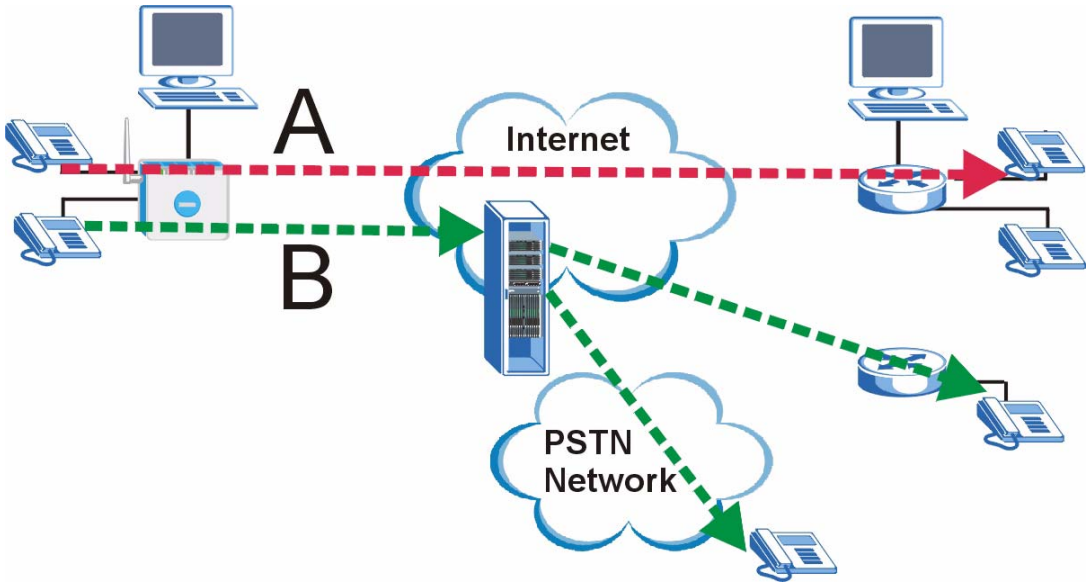
Use content filtering to block access to web sites with URLs containing keywords that you specify. You can define time periods and days during which content filtering is enabled and include or exclude particular computers on your network from content filtering. For example, you could block access to certain web sites for the kids.

1.1.2 Make Calls via Internet Telephony Service Provider

In a home or small office environment, you can use the ZyXEL Device to make and receive the following types of VoIP telephone calls:

- Peer-to-Peer calls (**A**) - Use the ZyXEL Device to make a call to the recipient's IP address without using a SIP proxy server.
- Calls via a VoIP service provider (**B**) - The ZyXEL Device sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones.

Figure 2 ZyXEL Device's VoIP Features



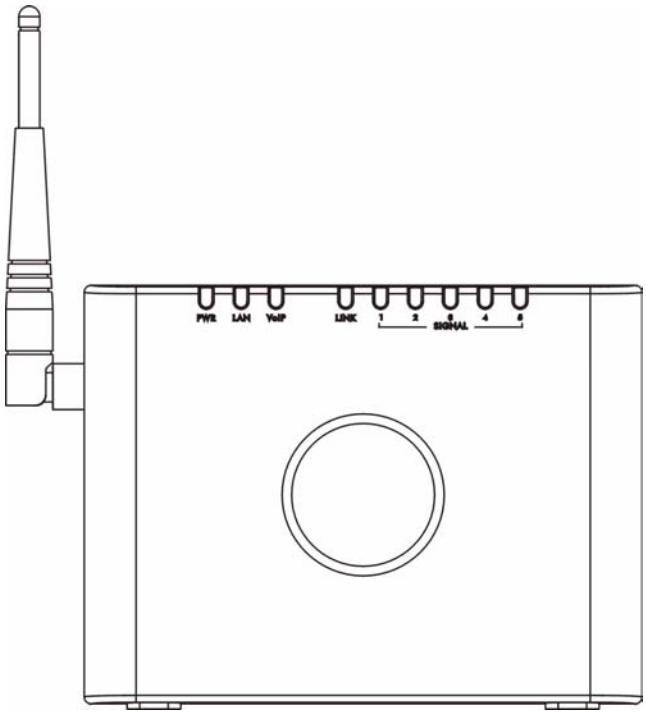
1.2 ZyXEL Device Hardware

Follow the instructions in the Quick Start Guide to make hardware connections.

1.2.1 LEDs

The following figure shows the LEDs (lights) on the ZyXEL Device.

Figure 3 The ZyXEL Device



The following table describes your ZyXEL Device's LEDs.

Table 2 The ZyXEL Device

LED	STATE	DESCRIPTION
PWR	OFF	The ZyXEL Device is not receiving power.
	RED	The ZyXEL Device is receiving power but has been unable to start up correctly. See the Troubleshooting section for more information.
	RED / ORANGE (BLINKING)	The ZyXEL Device is starting up.
	GREEN	The ZyXEL Device is receiving power and functioning correctly.
	GREEN (BLINKING)	The ZyXEL Device is performing a self-test.

Table 2 The ZyXEL Device

LED	STATE	DESCRIPTION
LAN	OFF	The LAN is not connected.
	GREEN	The ZyXEL Device has a successful Local Area Network (Ethernet) connection.
	GREEN (BLINKING)	Your device is sending/receiving data through the wireless LAN.
VoIP	OFF	No SIP account is registered, or the ZyXEL Device is not receiving power.
	GREEN	A SIP account is registered.
	GREEN (BLINKING)	A SIP account is registered, and the phone attached to the LINE port is in use (off the hook).
	ORANGE	A SIP account is registered and has a voice message.
	ORANGE (BLINKING)	A SIP account is registered and has a voice message, and the phone attached to the LINE port is in use (off the hook).
LINK	OFF	The ZyXEL Device is not connected to a wireless (WiMAX) network.
	GREEN	The ZyXEL Device is successfully connected to a wireless (WiMAX) network.
	GREEN (BLINKING SLOWLY)	The ZyXEL Device is searching for a wireless (WiMAX) network.
	GREEN (BLINKING QUICKLY)	The ZyXEL Device has found a wireless (WiMAX) network and is connecting.
SIGNAL 1 ~ 5	The SIGNAL LEDs display the Received Signal Strength Indication (RSSI) of the wireless (WiMAX) connection.	
	NO SIGNAL LEDS ON	There is no wireless connection.
	SIGNAL 1 ON	The signal strength is less than -80 dBm
	SIGNAL 2 ON	The signal strength is between -79 and -70 dBm
	SIGNAL 3 ON	The signal strength is between -69 and -60 dBm
	SIGNAL 4 ON	The signal strength is between -59 and -50 dBm
	SIGNAL 5 ON	The signal strength is between -49 and -30 dBm

1.2.2 Antenna

Connect the supplied 2dBi omni antenna to the SMA connector on the side of the ZyXEL Device. Alternatively, use a higher-powered antenna with a female SMA connector (not supplied) for improved signal reception.

The ZyXEL Device is equipped with an internal 6dBi directional patch antenna. If your signal strength is poor (use the **SIGNAL** LEDs to gauge received signal strength) orient the front of the ZyXEL Device (the side with the LEDs) towards the base station. If you do not know the location of the base station, experiment with moving the ZyXEL Device while observing the **SIGNAL** LEDs.

CHAPTER 2
Introducing the Web Configurator

This chapter describes how to access and navigate the web configurator.

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See the Troubleshooting chapter if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

1. Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "192.168.1.1" as the URL.
4. A password screen displays. The default password ("1234") displays in non-readable characters. If you haven't changed the password yet, you can just click **Login**. Click **Cancel** to revert to the default password in the password field. If you have changed the password, enter your password and click **Login**.

Figure 4 Password Screen

ZyXEL
MAX-200M1
Welcome to your router Configuration Interface
Enter your password and click "Login"
Password :
(max. 30 alphanumeric, printable characters and no spaces)
Note:
Please turn on the Javascript and ActiveX control setting on Internet Explorer when operating system is Windows XP and service pack is SP2.
Login
Cancel

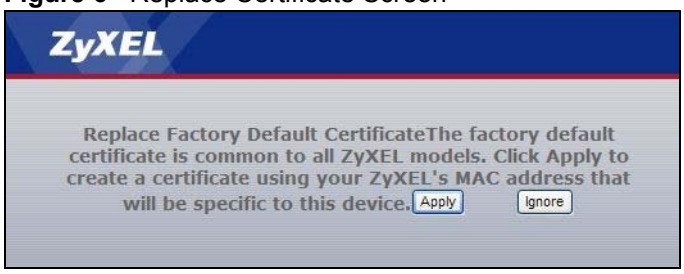
5 The following screen displays if you have not yet changed your password. It is highly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.

Figure 5 Change Password Screen

ZyXEL
Please enter a new password
Your router is currently using the default password. To protect your network from unauthorized users we suggest you change your password at this time. Please select a new password that will be easy to remember yet difficult for others to guess.We suggest you combine text with numbers to make it more difficult for an intruder to guess.
The administrator password should must be between 1 - 30 characters.
New Password:
Retype to Confirm:
Apply
Ignore

6 Click **Apply** in the next screen to create a certificate using your ZyXEL Device's MAC address that will be specific to this device. This certificate is used for authentication when using a secure HTTPS connection over the Internet.

Figure 6 Replace Certificate Screen


ZyXEL
Replace Factory Default CertificateThe factory default certificate is common to all ZyXEL models. Click Apply to create a certificate using your ZyXEL's MAC address that will be specific to this device.
Apply
Ignore

7 A screen displays to let you choose whether to go to the wizard or the advanced screens.

- Click **Go to Wizard setup** if you are logging in for the first time or if you want to make basic changes. The wizard selection screen appears after you click **Apply**. See Chapter 4 on page 49 for more information.
- Click **Go to Advanced setup** if you want to configure features that are not available in the wizards. The main screen appears after you click **Apply**. See Section 2.2 on page 36 for more information.
- Click **Exit** if you want to log out.

Note: For security reasons, by default the ZyXEL Device automatically logs you out if you do not use the web configurator for five minutes. If this happens, log in again.

Figure 7 Wizard or Advanced Screen

ZyXEL
Please select Wizard or Advanced mode
The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.
Use Advanced mode if you need access to more advanced features not included in Wizard mode.
Go to Wizard setup
Go to Advanced setup
Exit

2.1.2 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to "1234".

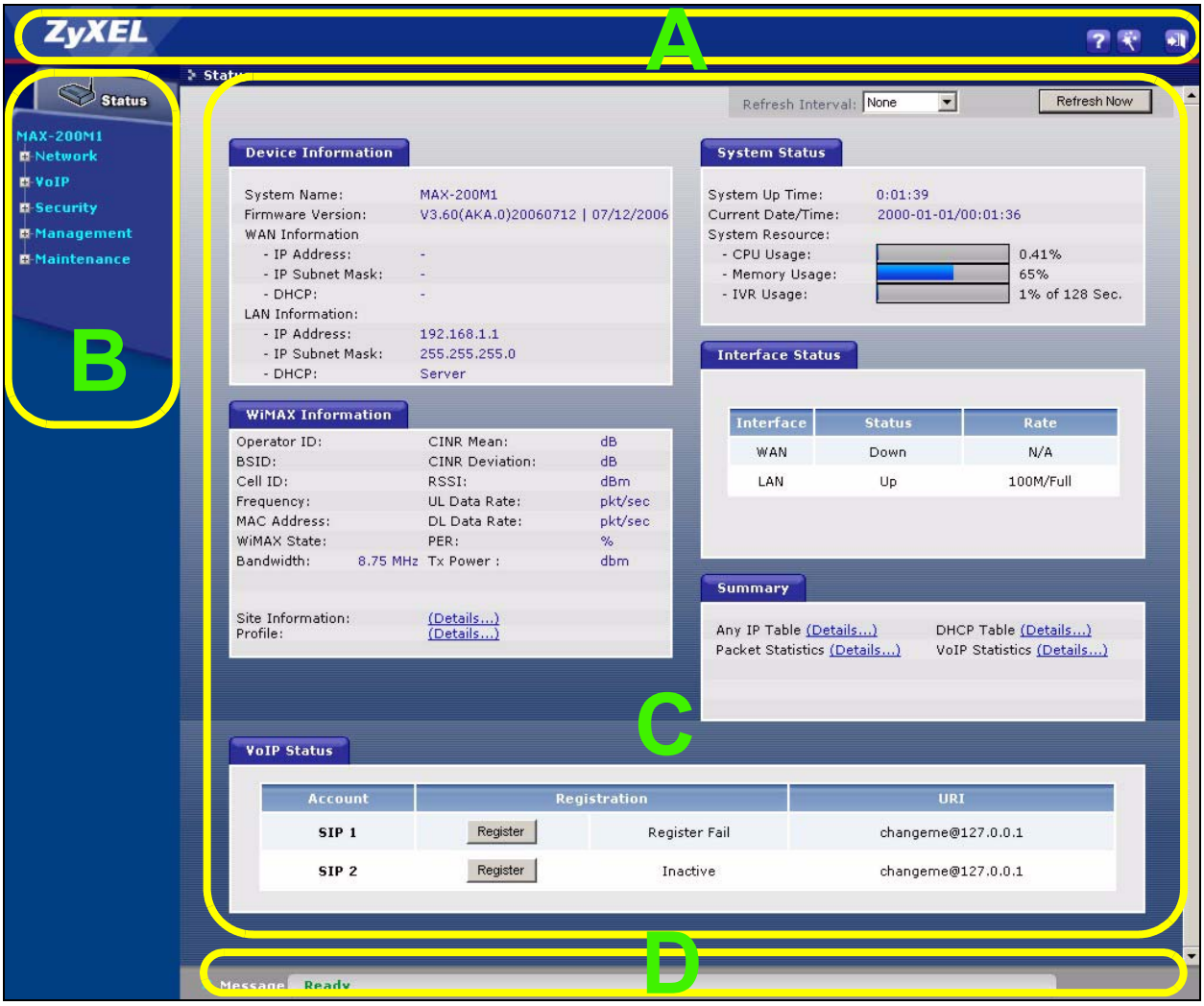
2.1.2.1 Using The Reset Button

1 Make sure the **POWER** light is on (not blinking).

2 To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** light begins to blink and then release it. When the **POWER** light begins to blink, the defaults have been restored and the device restarts.

2.2 Web Configurator Main Screen

Figure 8 Main Screen



As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window
- **D** - status bar

2.2.1 Title Bar

The title bar provides some icons in the upper right corner.

The icons have the following functions.

Table 3 Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
	Wizards: Click this icon to go to the configuration wizards. See Chapter 4 on page 49 for more information.
	Logout: Click this icon to log out of the web configurator.

2.2.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure ZyXEL Device features. The following table describes the menu items.

Table 4 Navigation Panel Summary

LINK	TAB	FUNCTION
Status		This screen contains administrative and system-related information.
Network		
WAN	Internet Connection	Use this screen to configure ISP parameters, WAN IP address assignment and other advanced properties.
	WiMAX Frequency	Use this screen to set the radio frequencies the ZyXEL Device searches for a WiMAX connection.
	Advanced	Use this screen to configure DNS servers, RIP & Multicast, and Windows networking settings.
	Traffic Redirect	Use this screen to configure your traffic redirect properties
LAN	IP	Use this screen to configure LAN TCP/IP settings.
	DHCP Setup	Use this screen to configure LAN DHCP and DNS settings.
	Static DHCP	Use this screen to always assign specific IP addresses to individual MAC addresses.
	Client List	Use this screen to view current DHCP client information.
	IP Alias	Use this screen to partition your LAN interface into subnets.
	Advanced	Use this screen to enable Any IP
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Trigger Port	Use this screen to set port triggering rules.
	ALG	Use this screen to configure Application Level Gateway settings.
VoIP		
SIP	SIP Settings	Use this screen to configure your ZyXEL Device's Voice over IP settings.
	QoS	Use this screen to configure your ZyXEL Device's Quality of Service settings for VoIP.
Phone	Analog Phone	Use this screen to set which SIP account to use for outgoing or incoming calls.
	Common	Use this screen to configure general phone settings.
	Region	Use this screen to select your location and call service mode.

Table 4 Navigation Panel Summary

LINK	TAB	FUNCTION
Phone Book	Incoming Call Policy	Use this screen to configure call-forwarding.
	Speed Dial	Use this screen to configure speed dial for SIP phone numbers that you call often.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall and the default action to take on network traffic going in specific directions.
	Services	Use this screen to set the days and times for your device to perform service blocking.
Content Filter	Filter	Use this screen to block sites containing certain keywords in the URL, exclude a range of users on the LAN from content filtering on your ZyXEL Device and restrict certain web features.
	Schedule	Use this screen to set the days and times for your ZyXEL Device to perform content filtering.
Management		
Static Route	IP Static Route	Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes.
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the ZyXEL Device.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the ZyXEL Device.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the ZyXEL Device.
	SNMP	Use this screen to configure your ZyXEL Device's settings for Simple Network Management Protocol management.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the ZyXEL Device.
	Security	Use this screen to set whether or not your device will respond to pings and probes for services that you have not made available.
UPnP	General	Use this screen to turn UPnP on or off.
Maintenance		
System	General	This screen contains administrative and system-related information and also allows you to change your password.
	Dynamic DNS	Use this screen to set up Dynamic DNS.
	Time Setting	Use this screen to change your ZyXEL Device's time and date.
Logs	View Log	Use this screen to display your device's logs.
	Log Settings	Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you.
Tools	Firmware	Use this screen to upload firmware to your device.
	Configuration	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
	Restart	This screen allows you to reboot the ZyXEL Device without turning the power off.

2.2.3 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See Chapter 6 on page 59 for more information about the **Status** screen.

2.2.4 Status Bar

Check the status bar when you click **Apply** or **OK** to verify that the configuration has been updated.

CHAPTER 3
Tutorial

This chapter provides examples showing how to use the ZyXEL Device to access the Internet, set up VoIP and make a telephone call over the Internet using the ZyXEL Device's speed dial feature.

3.1 Connect to the Internet

This section shows how to set up your Internet access details on the ZyXEL Device and configure your WiMAX frequency settings. See Section 7.2 on page 71 for more information on how WiMAX works.

3.1.1 Configure Internet Access Settings

To access the Internet, you need information from your Internet Service Provider (ISP) about your account and the network. In this example, your user name is 'User1234' and your password is '4321'.

Your ISP has also told you that you will be assigned a dynamic IP address each time you connect to the Internet. See Section 7.3 on page 72 for more details about dynamic and static IP addresses.

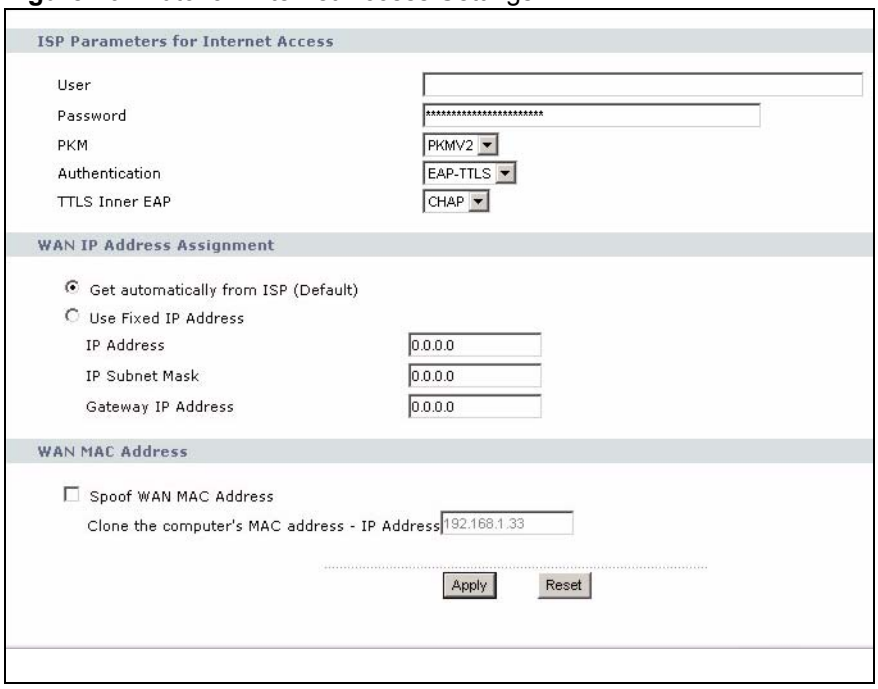
Once you have connected the ZyXEL Device to your computer and accessed the Web Configurator (see the Quick Start Guide for details) follow the steps below to connect to a network.

1 In the Web Configurator, click **Network > WAN** in the navigation panel.

Figure 9 Tutorial: Navigation Panel

2 The following screen displays. This screen is where you enter your Internet access details.

Figure 10 Tutorial: Internet Access Settings



In the **ISP Parameters for Internet Access** area, enter your username ('User1234') in the **User** field, and enter your password ('4321') in the **Password** field. Your ISP gave no information about the other fields in this section, so leave them at their defaults.

In the **WAN IP Address Assignment** area, make sure that **Get Automatically from ISP (Default)** is selected. Leave all other fields at their default values.

3 Click **Apply**. Your Internet access settings are saved to the ZyXEL Device, and are used automatically each time you connect to the Internet.

3.1.2 Configure WiMAX Settings

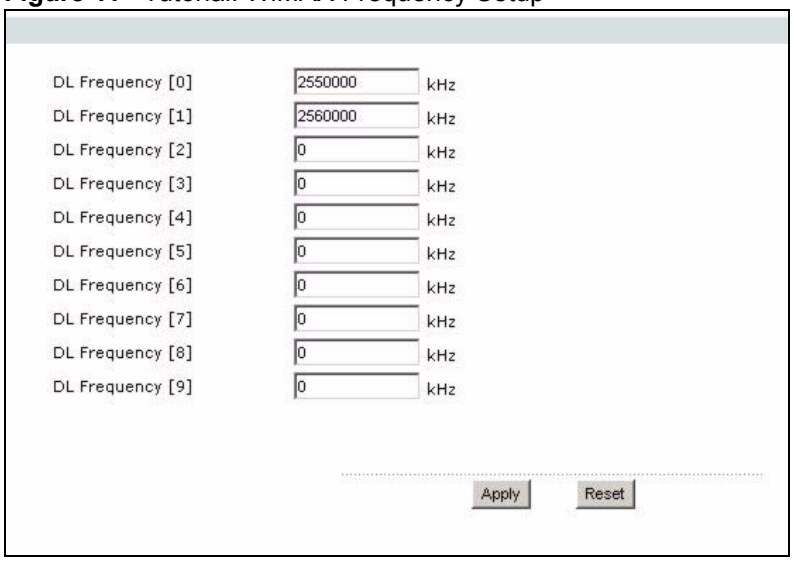
The **WiMAX Frequency** screen allows you to specify a set of frequencies to search for a connection to a base station. Before you start, you need information from your ISP about the supported frequencies.

In this example, your ISP has told you that the supported WiMAX frequencies are at 2.55 and 2.56 Gigahertz (GHz). See Section 7.4 on page 74 for more information on radio frequencies.

Follow the steps below to configure your frequency settings.

1 Click **Network > WAN > WiMAX Frequency** to open the screen shown next.

Figure 11 Tutorial: WiMAX Frequency Setup


DL Frequency [0] 2550000 kHz
DL Frequency [1] 2560000 kHz
DL Frequency [2] 0 kHz
DL Frequency [3] 0 kHz
DL Frequency [4] 0 kHz
DL Frequency [5] 0 kHz
DL Frequency [6] 0 kHz
DL Frequency [7] 0 kHz
DL Frequency [8] 0 kHz
DL Frequency [9] 0 kHz
Apply
Reset

2 Enter the frequency settings your ISP gave you in the **DL Frequency** fields. Note that these fields are in kilohertz (**kHz**).

2.55 GHz is equal to 2550000 kHz, so enter **2550000** in the DL Frequency [0] field.

2.56 GHz is equal to 2560000 kHZ, so enter **2560000** in the DL Frequency [1] field.

3 Click **Apply** to save your settings. The ZyXEL Device scans for an available wireless connection at the **DL Frequency [0]** setting (2.55 GHz) and, if it does not find an available connection, searches at the **DL Frequency [1]** setting (2.56 GHz). When it finds an available connection, the fields in this screen will be automatically set to use that frequency.

For an example of using the WiMAX Frequency screen to configure more frequencies, see Section 7.4.2.1 on page 77.

4 Look at the LEDs on your ZyXEL Device. When the ZyXEL Device successfully connects to a base station, the **LINK** LED shines green steadily. The **SIGNAL 1 ~ 5** LEDs indicate the signal strength, with **SIGNAL 5** showing a very strong signal and **SIGNAL 1** showing a very weak signal.

5 Open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured. If you cannot access the web site, check the Troubleshooting section of this User's Guide.

3.2 Make a Telephone Call Over the Internet

To make a call over the Internet using the ZyXEL Device, first do the following things:

- Set up hardware connections from the ZyXEL Device to your computer, your telephone and the power supply (see the Quick Start Guide for more details on hardware connections).
- Set up your Internet access and WiMAX settings on the ZyXEL Device (see Section 3.1.1 on page 41 and Section 3.1.2 on page 42 for examples).
- Set up an account with a Voice over IP (VoIP) provider. This account (called a SIP account) allows you to make calls over the Internet. See Chapter 10 on page 105 for more information on SIP accounts.

Use the sections below to set up your SIP account and speed dialing, and place a VoIP call.

3.2.1 Configure Your SIP Account

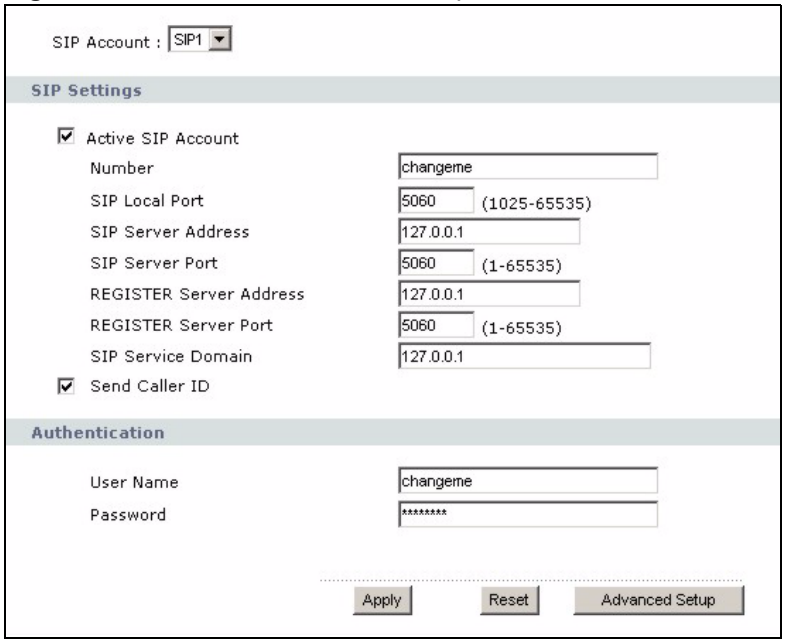
Your ZyXEL Device needs to be configured with the details of your SIP account before you can use it to make calls over the Internet. In this example, your SIP identity is "id123@abcvoip.com", your user name is "id123" and your password is "zyx987". Your VoIP provider has told you that the SIP server address is "sipserver-abcvoip.com". See Section 10.1.3 on page 105 for more information on SIP identities.

Once you have connected the ZyXEL Device to your computer and accessed the Web Configurator (see the Quick Start Guide for details) follow the steps below to configure your SIP settings.

1 In the Web Configurator, click **VoIP > SIP** in the navigation panel.

The following screen displays. This screen is where you enter your SIP account details.

Figure 12 Tutorial: SIP Account Setup



2 Select **SIP1** from the **SIP Account** list and make sure that the **Active SIP Account** box is selected.

3 Enter your SIP user name ('id123') in the **Number** field.

4 Enter your VoIP provider's SIP server name ('sipserver-abcvoip.com') in the **SIP Server Address** field. As your VoIP provider did not give you a different **REGISTER Server Address**, enter 'sipserver-abcvoip.com' again.

Enter your VoIP provider's domain name ('abcvoip.com') in the **SIP Service Domain** field.

5 In the Authentication area, enter 'id123' in the **User Name** field, and 'zyx987' in the **Password** field. Leave the **SIP Local Port**, **SIP Server Port** and **REGISTER Server Port** fields at their default values, as your VoIP provider did not supply port details.

Click **Apply**.

6 Click on the **Status** button in the navigation panel to check that your SIP account is correctly registered.

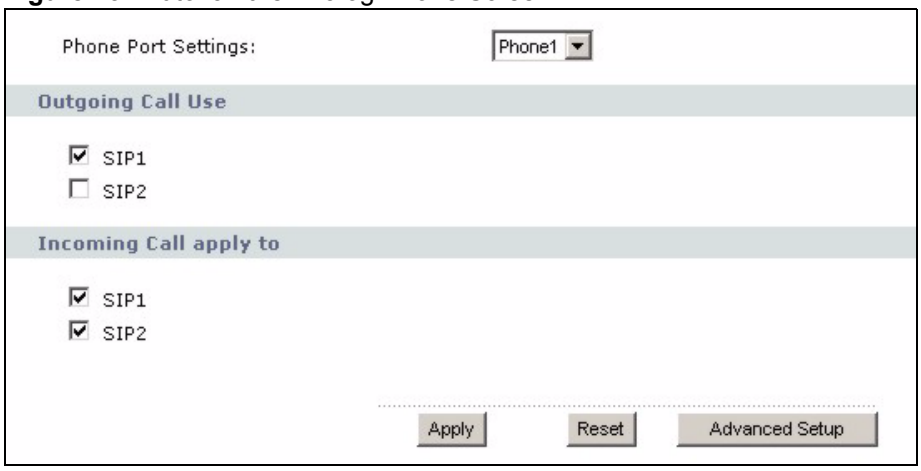
Look in the **VoIP Status** area towards the bottom of the **Status** screen. If the **SIP 1** account displays **Registered** in the **Registration** field, it is ready to use.

If the **Registration** field for the **SIP 1** account displays **Register Fail** or **Inactive**, click the **Register** button, check your settings in the **VoIP > SIP** screen or contact your VoIP provider to confirm that you have the correct settings and that your account is active.

3.2.2 Configure a Phone

Once you have set up your SIP account, click **VoIP > Phone > Analog Phone** in the navigation panel. The following screen displays.

Figure 13 Tutorial: the Analog Phone Screen



Use this screen to make sure that the phone connected to your ZyXEL Device uses the correct SIP account.

1 Select **Phone1** from the drop-down list box.

2 In the **Outgoing Call Use** area, select **SIP1**.

3 In the **Incoming Call apply to** area, select both **SIP1** and **SIP2**.

4 Click **Apply**. Your analog phone settings are saved.

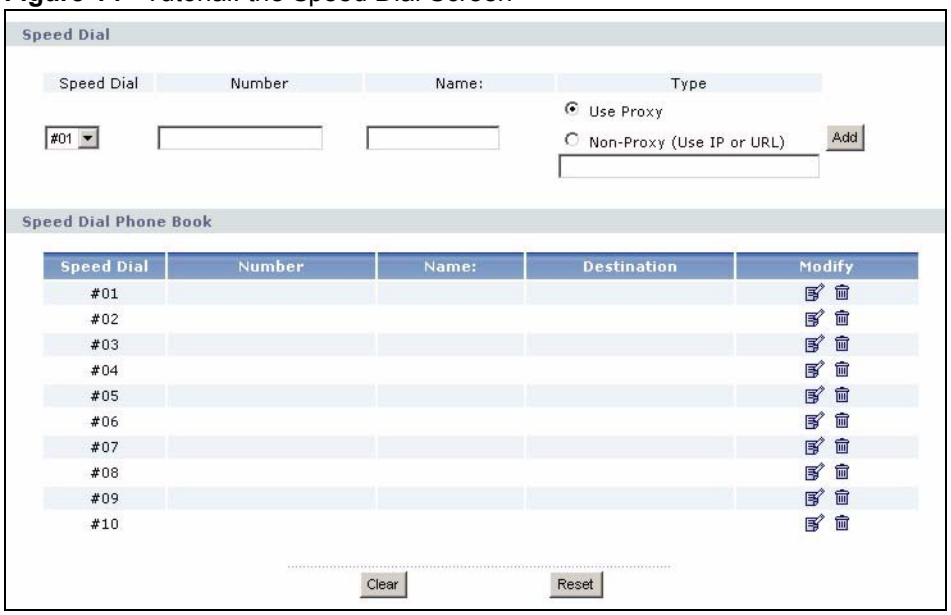
3.2.3 Set Up Speed Dialing and Make a Call

In this example you want to set up speed dialling to make calls to a friend, Bob, whose SIP account number is 2345@xyzvoip.com. Your voIP provider, abcvoip.com, has told you that to call an xyzvoip.com number you must add '555' at its start.

Note: Different VoIP providers implement calls to other networks in different ways. Check with your provider for details.

To configure speed dialling on the ZyXEL Device, click **VoIP > Phone Book > Speed Dial**. The following screen displays.

Figure 14 Tutorial: the Speed Dial Screen



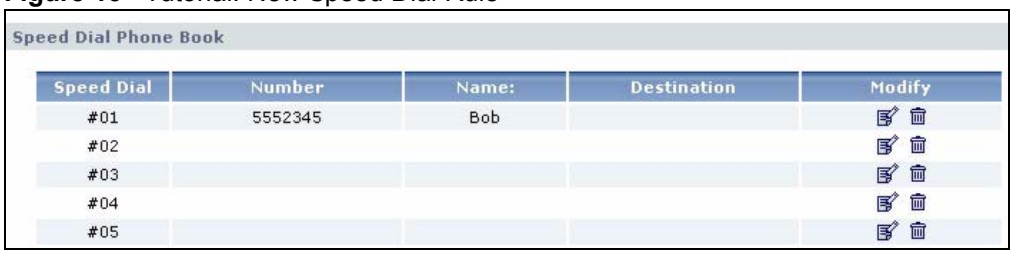
Use the following steps to set up a speed dial entry.

1 You can have up to ten speed dial rules. Select the rule number (**1**, in this example) from the **Speed Dial** drop-down list box.

2 In the **Number** field, enter "5552345" and in the **Name** field enter "Bob". Under **Type**, select **Use Proxy** and click **Add**.

The new speed dial rule is displayed in the **Speed Dial Phone book List**.

Figure 15 Tutorial: New Speed Dial Rule



Use the following steps to call a number from the speed dial list.

1. Ensure that your phone is correctly connected to the ZyXEL Device. See the Quick Start Guide for details of hardware connections.
2. Lift the phone's receiver and type the speed dial number exactly as it appears in the **Speed Dial Phone Book** list. In this case, Bob's phone number occupies rule #01, so dial "#01" on the phone's keypad to make the call.

CHAPTER 4
Internet Setup Wizard

This chapter provides information on the wizard setup screens for Internet access.

4.1 Wizard Setup Overview

The wizard will guide you through several steps. You will need to enter some information for identification purposes, then the wizard will guide you through configuring your Internet settings.

4.2 Internet Connection Wizard Setup

1 After you enter the password to access the web configurator, select **Go to Wizard setup**. Otherwise, click the wizard icon ( ) in the top right corner of the web configurator to go to the wizards.

Figure 16 Select a Mode

Welcome to the ZyXEL Wizard Setup
CONNECTION WIZARD
The connection wizard will walk you through the most common configuration options. This wizard has been broken down into two steps, each of which may have multiple pages.
VOIP SETUP

2 Click **CONNECTION WIZARD** to configure the system for Internet access.

3 The following screen displays. Click **Next** to continue. Click **Back** at any time to return to the previous screen, or **Exit** to leave the wizard setup.

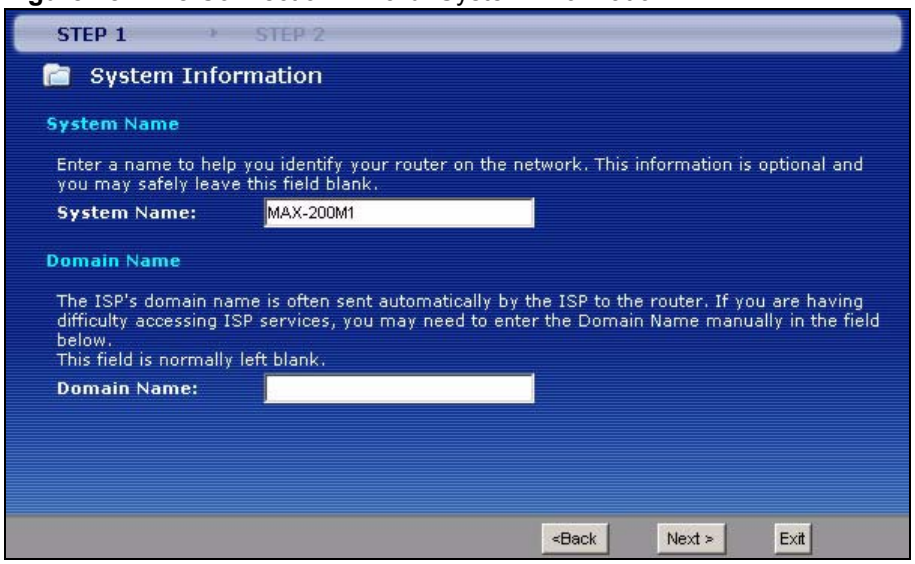
Figure 17 Connection Wizard: Introduction

Welcome to the ZyXEL Connection Wizard
The Connection Wizard will walk you through the most common configuration options. This wizard has been broken down into three steps, each of which may have multiple pages.
This wizard will take you through the following steps:
Step 1 : System Information Setup.
Step 2 : Internet Configuration Setup.
<Back
Next >
Exit

4 In the next screen you can give your ZyXEL Device a name (optional) in the **System Name** field. Enter up to thirty letters (this field is case-sensitive) or numbers. The 'at' symbol (@), dash (-), underscore (_) and period (.) are also permitted.

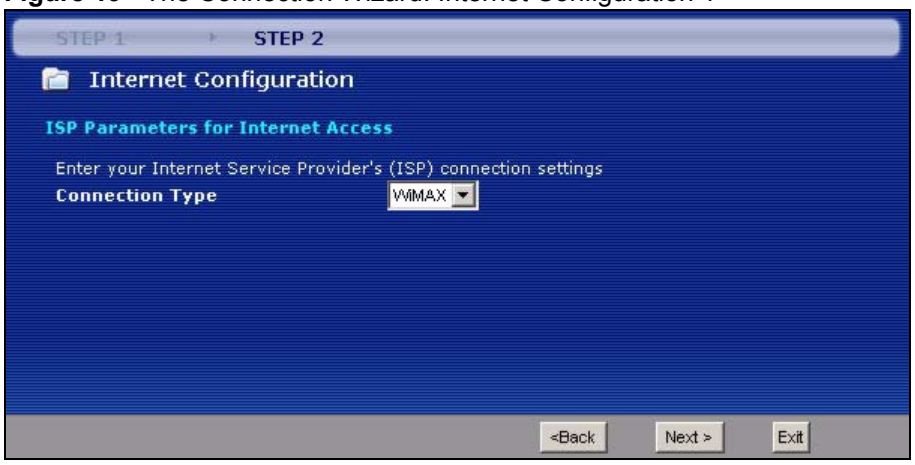
Enter your ISP's IP address in the **Domain Name** field if your ISP has instructed you to do so, or if you are having trouble accessing the Internet. Otherwise, leave this field blank.

Figure 18 The Connection Wizard: System Information


STEP 1
STEP 2
System Information
System Name
Enter a name to help you identify your router on the network. This information is optional and you may safely leave this field blank.
System Name:
MAX-200M1
Domain Name
The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below.
This field is normally left blank.
Domain Name:
<Back
Next >
Exit

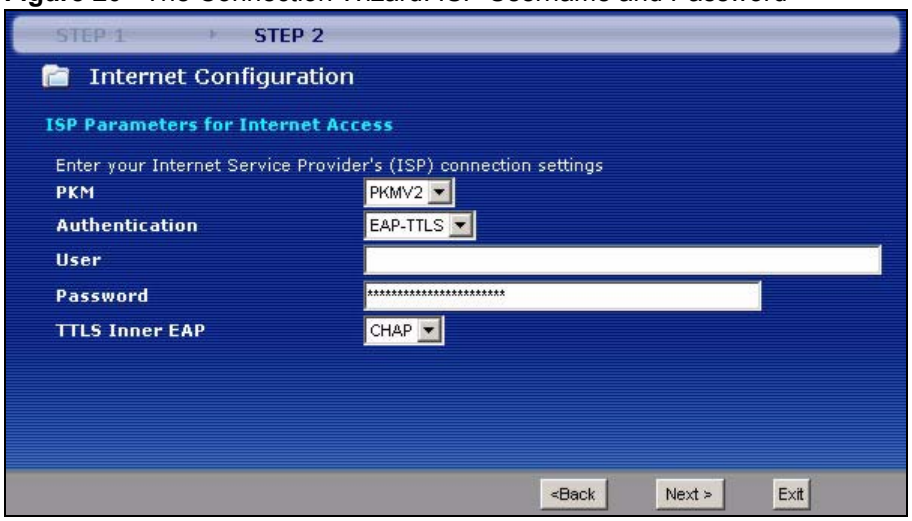
5 The following screen appears. Leave the **Connection Type** at the default setting and click **Next**.

Figure 19 The Connection Wizard: Internet Configuration 1



6 Enter your Internet account information (username and password) exactly as provided by your ISP. Leave the **PKM**, **Authentication** and **TTLS Inner EAP** fields at their default settings. Click **Next** to continue.

Figure 20 The Connection Wizard: ISP Username and Password



7 A fixed IP address is a static IP that your ISP gives you. An automatic (dynamic) IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.

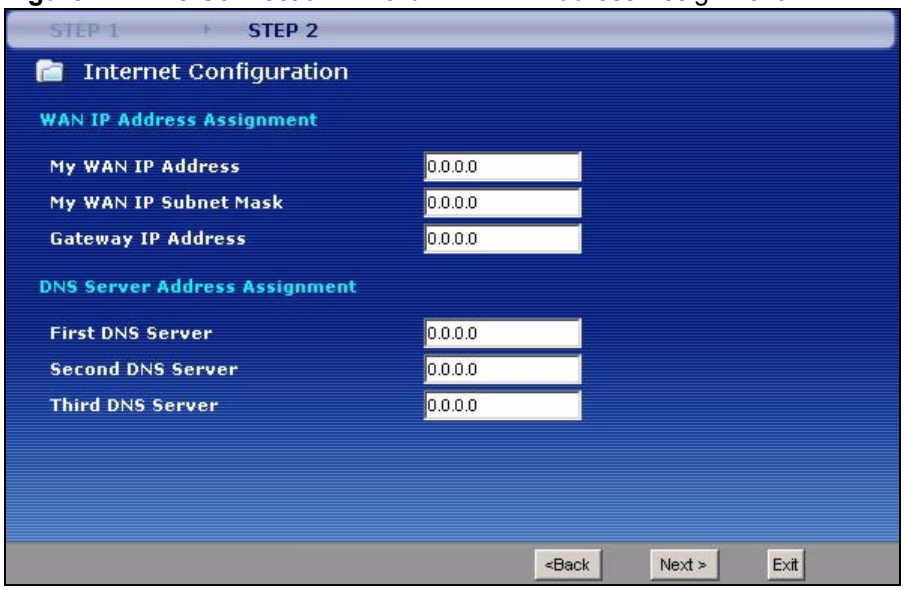
In the following screen, select **Use fixed IP address provided by your ISP** if your ISP gave you an IP address to use. Otherwise, select **Get automatically from your ISP**.

Figure 21 The Connection Wizard: Your IP Address

8 If you selected **Get automatically from your ISP** in the previous screen, skip this step. If you selected **Use fixed IP address provided by your ISP**, the following screen appears.

Enter your IP address, subnet mask, gateway address and DNS details exactly as they were given to you by your ISP.

Figure 22 The Connection Wizard: WAN IP Address Assignment

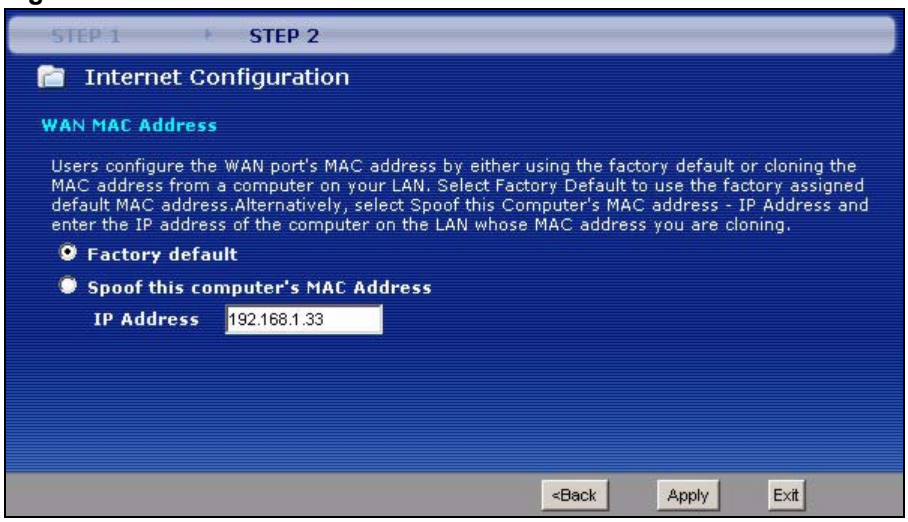


9 Every network device has a unique, factory-assigned Media Access Control (MAC) address. A device's MAC address can be used to identify it over the network. In the following screen, you can set the ZyXEL Device to transmit its own MAC address over the Internet, or to use the MAC address of another device connected to the ZyXEL Device ("spoofing").

Leave **Factory Default** selected to have the ZyXEL Device use its own MAC address, or select **Spoof this computer's MAC address** to use another.

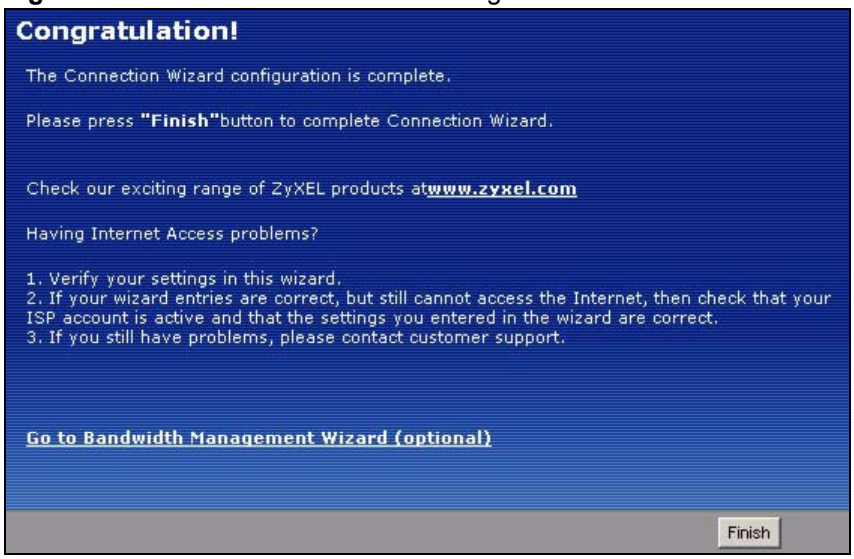
The **IP Address** field contains the IP address of the computer you are using to configure the ZyXEL Device by default. If you have multiple devices connected to the ZyXEL Device, you can enter the IP address of another device on the LAN to have the ZyXEL Device use its MAC address instead. Click **Apply** to move on to the final screen.

Figure 23 The Connection Wizard: WAN MAC Address


STEP 1
STEP 2
Internet Configuration
WAN MAC Address
Users configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Select Factory Default to use the factory assigned default MAC address.Alternatively, select Spoof this Computer's MAC address - IP Address and enter the IP address of the computer on the LAN whose MAC address you are cloning.
Factory default
Spoof this computer's MAC Address
IP Address
192.168.1.33
<Back
Apply
Exit

10 Click **Finish** to complete and save the Connection Wizard settings.

Figure 24 The Connection Wizard: Congratulations


Congratulation!
The Connection Wizard configuration is complete.
Please press "Finish"button to complete Connection Wizard.
Check our exciting range of ZyXEL products atwww.zyxel.com
Having Internet Access problems?
1. Verify your settings in this wizard.
2. If your wizard entries are correct, but still cannot access the Internet, then check that your ISP account is active and that the settings you entered in the wizard are correct.
3. If you still have problems, please contact customer support.
Go to Bandwidth Management Wizard (optional)
Finish

11 Launch your web browser and navigate to www.zyxel.com. Internet access is just the beginning. Refer to the rest of this guide for more detailed information on the complete range of ZyXEL Device features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the wizard setup are correct.

CHAPTER 5
VoIP Wizard

This chapter shows you how to use the wizard to set up your SIP account(s).

5.1 Introduction

The ZyXEL Device has Voice over IP (VoIP) communication capabilities that allow you to use a traditional analog telephone to make Internet calls. You can configure the ZyXEL Device to use up to two SIP based VoIP accounts.

5.2 VOIP Wizard Setup

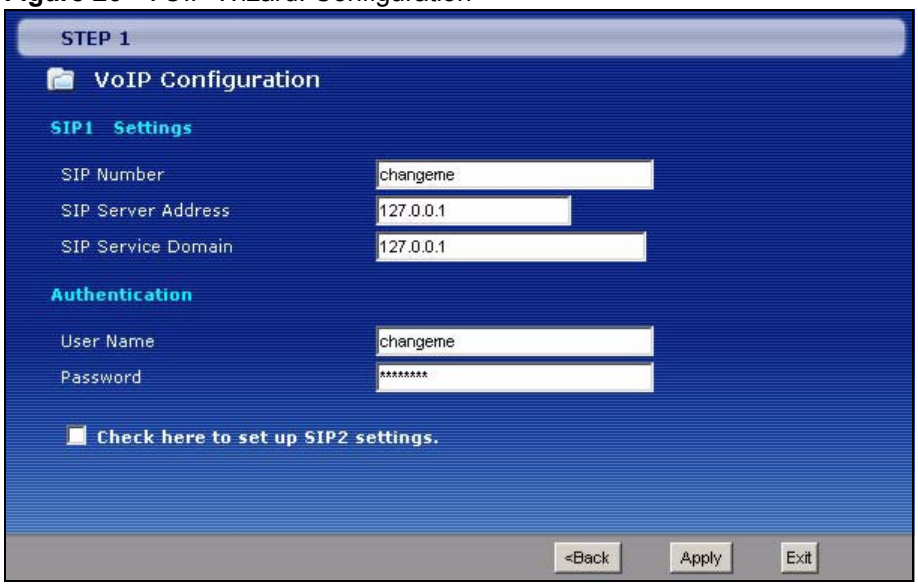
1 After you enter the password to access the web configurator, select **Go to Wizard setup**. Otherwise, click the wizard icon ( ) in the top right corner of the web configurator to display the wizard main screen. Click **VOIP SETUP** to configure the system for Voice Over Internet connection.

Figure 25 Select a Mode

Welcome to the ZyXEL Wizard Setup
CONNECTION WIZARD
The connection wizard will walk you through the most common configuration options. This wizard has been broken down into two steps, each of which may have multiple pages.
VOIP SETUP

2 The following screen displays. This wizard screen allows you to configure your voice settings for SIP account 1. Fill in the fields with information from your VoIP service provider. Leave the default settings in fields for which no information was provided (except if otherwise specified). See Chapter 10 on page 105 for background information on these fields.

Figure 26 VOIP Wizard: Configuration



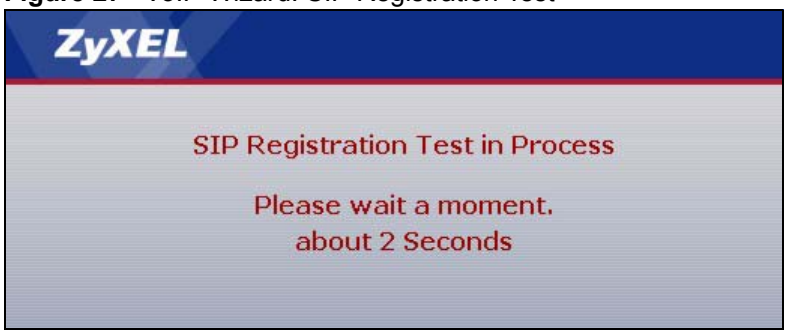
The following table describes the labels in this screen

Table 5 VOIP Wizard Configuration

LABEL	DESCRIPTION
SIP Number	Enter your SIP number in this field (use the number or text that comes before the @ symbol in a SIP account like 1234@VoIP-provider.com). You can use up to 127 ASCII characters.
SIP Server Address	Type the IP address or domain name of the SIP server in this field. It doesn't matter whether the SIP server is a proxy, redirect or register server. You can use up to 95 ASCII characters.
SIP Service Domain	Enter the SIP service domain name in this field (the domain name that comes after the @ symbol in a SIP account like 1234@VoIP-provider.com). You can use up to 127 ASCII Extended set characters.
User Name	This is the user name for registering this SIP account with the SIP register server. Type the user name exactly as it was given to you. You can use up to 95 ASCII characters.
Password	Type the password associated with the user name above. You can use up to 95 ASCII Extended set characters.
Check here to set up SIP2 settings.	This screen configures SIP account 1. Select the check box if you have a second SIP account that you want to use. You will need to configure the same fields for the second SIP account.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to complete the wizard setup and save your configuration.
Exit	Click **Exit** to close the wizard without saving your settings.

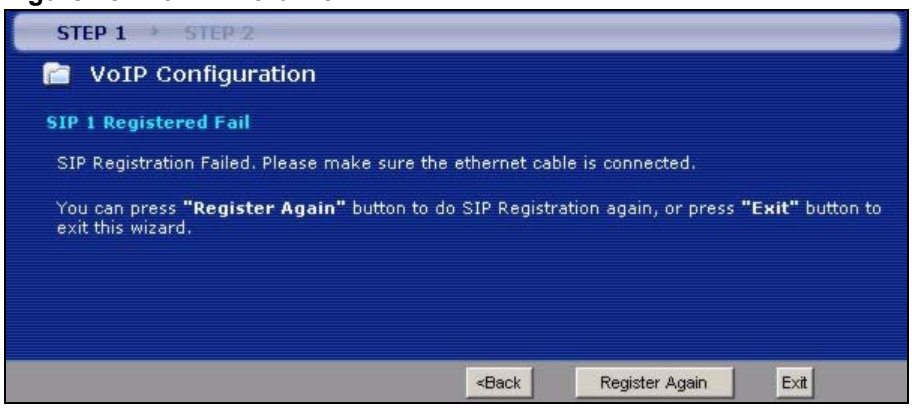
3 The ZyXEL Device attempts to register your SIP account with the SIP server.

Figure 27 VoIP Wizard: SIP Registration Test



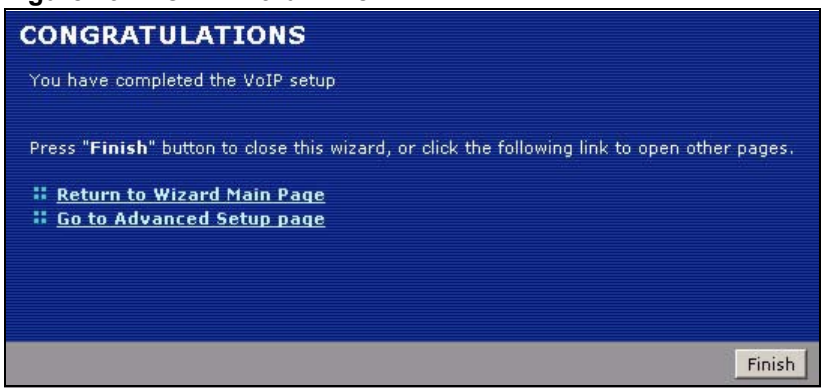
4 This screen displays if SIP account registration fails. Check your WiMAX connection using the **LINK** and **SIGNAL** LEDs on the front of the ZyXEL Device. Then wait a few seconds and click **Register Again**. If your Internet connection was already working, you can click **Back** and try re-entering your SIP account settings.

Figure 28 VoIP Wizard: Fail


STEP 1 STEP 2
VoIP Configuration
SIP 1 Registered Fail
SIP Registration Failed. Please make sure the ethernet cable is connected.
You can press "Register Again" button to do SIP Registration again, or press "Exit" button to exit this wizard.
<Back
Register Again
Exit

5 This screen displays if your SIP account registration was successful. Click **Return to Wizard Main Page** if you want to use another configuration wizard. Click **Go to Advanced Setup page** or **Finish** to close the wizard and go to the main web configurator screens.

Figure 29 VOIP Wizard: Finish


CONGRATULATIONS
You have completed the VoIP setup
Press "Finish" button to close this wizard, or click the following link to open other pages.
Return to Wizard Main Page
Go to Advanced Setup page
Finish

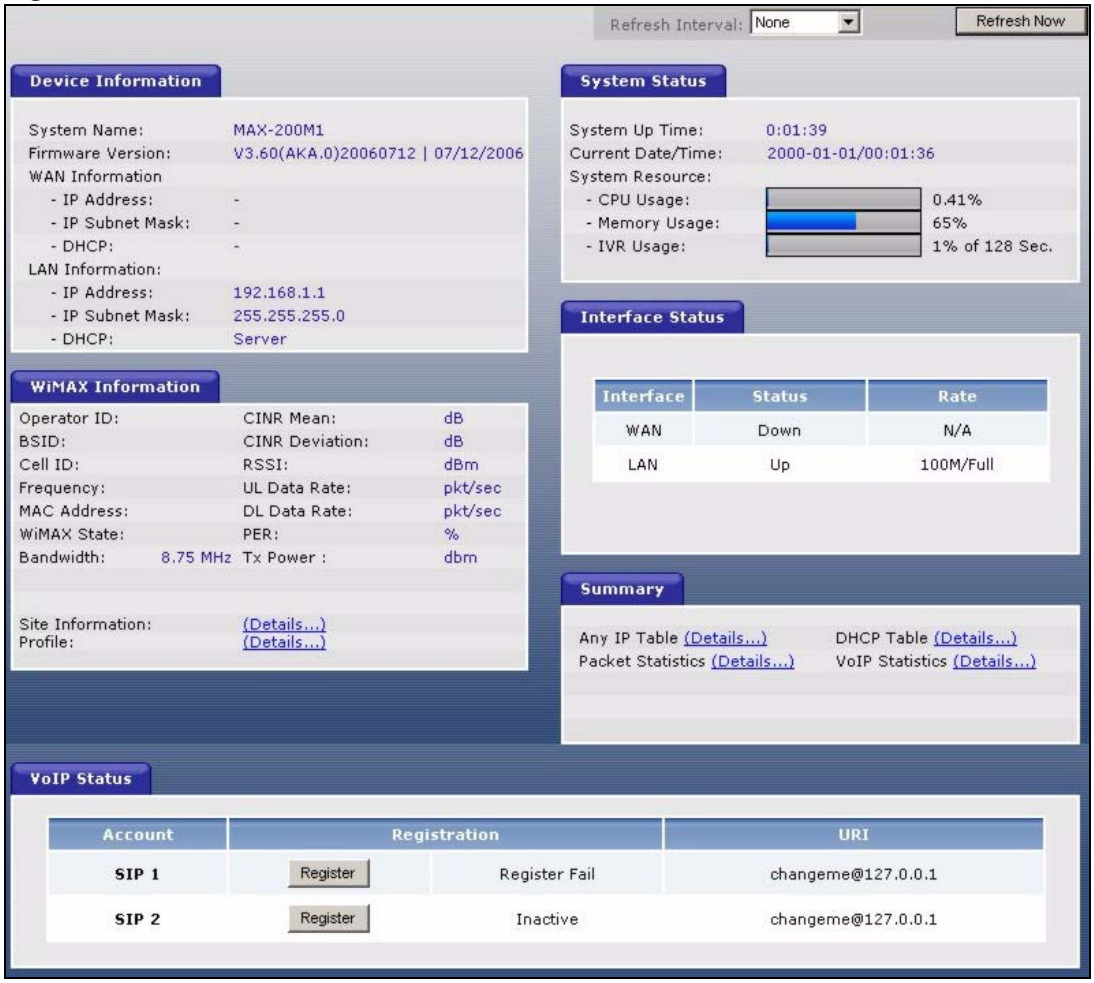
CHAPTER 6
Status Screens

Use the **Status** screens to look at the current status of the device, system resources, interfaces (LAN and WAN), and SIP accounts. You can also register and unregister SIP accounts. The **Status** screen also provides detailed information from Any IP and DHCP and statistics from WiMAX, VoIP, bandwidth management, and traffic.

6.1 Status Screen

Click **Status** to open this screen.

Figure 30 Status Screen



Each field is described in the following table.

Table 6 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the ZyXEL Device to update this screen.
Refresh Now	Click this to update this screen immediately.
Device Information	
System Name	This field displays the ZyXEL Device system name. It is used for identification. You can change this in the **Maintenance > System > General** screen's **System Name** field.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. You can change the firmware version by uploading new firmware in **Maintenance > Tools > Firmware**.
WAN Information	
IP Address	This field displays the current IP address of the ZyXEL Device in the WAN.
IP Subnet Mask	This field displays the current subnet mask on the WAN.
DHCP	This field displays what DHCP services the ZyXEL Device is using in the WAN. Choices are: **Client** - The ZyXEL Device is a DHCP client in the WAN. Its IP address comes from a DHCP server on the WAN. **None** - The ZyXEL Device is not using any DHCP services in the WAN. It has a static IP address. If you are not using Roadrunner on Ethernet, you can change this in **Network > WAN**. If you are using Roadrunner on Ethernet, this is controlled by Roadrunner.
LAN Information	
IP Address	This field displays the current IP address of the ZyXEL Device in the LAN.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP	This field displays what DHCP services the ZyXEL Device is providing to the LAN. Choices are: **Server** - The ZyXEL Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The ZyXEL Device is routing DHCP requests to one or more DHCP servers. The DHCP server(s) may be on another network. **None** - The ZyXEL Device is not providing any DHCP services to the LAN. You can change this in **Network > LAN > DHCP Setup**.
WiMAX Information	
Operator ID	Every WiMAX service provider has a unique Operator ID number, which is broadcast by each base station it owns. You can only connect to the Internet through base stations belonging to your service provider's network.
BSID	This field displays the identification number of the wireless base station to which the ZyXEL Device is connected. Every base station transmits a unique BSID, which identifies it across the network.
Cell ID	A base station's coverage area can be divided into multiple cells. This field shows the identification number of the cell in which the ZyXEL Device is connected.
Frequency	This field displays the radio frequency of the ZyXEL Device's wireless connection to a base station.

Table 6 Status Screen

LABEL	DESCRIPTION
MAC address	This field displays the Media Access Control address of the ZyXEL Device. Every network device has a unique MAC address which identifies it across the network.
WiMAX State	This field displays the status of the ZyXEL Device's current connection. • **NA**: the ZyXEL Device is starting up. • **Fail**: The ZyXEL Device is unable to connect to a base station. • **Initial Synchronization**: the ZyXEL Device is attempting to locate a base station. • **Initial DCD** (Downlink Channel Descriptor): the ZyXEL Device has located a base station and is receiving information about a possible downlink connection. • **Initial UCD** (Uplink Channel Descriptor): the ZyXEL Device is receiving information from the base station about a possible uplink connection. • **Initial Ranging and Calibration**: the ZyXEL Device and the base station are transmitting and receiving information about the distance between them. Ranging allows the ZyXEL Device to use a lower transmission power level when communicating with a nearby base station, and a higher transmission power level when communicating with a distant base station. • **Initial Negotiation**: the ZyXEL Device and the base station are exchanging information about their capabilities. • **Initial PKM** (Privacy Key Management): the ZyXEL Device and the base station are exchanging security information. • **Initial Registration**: the ZyXEL Device is registering with a RADIUS server. • **Running**: the ZyXEL Device has successfully registered with the base station. Traffic can now flow between the ZyXEL Device and the base station. • **Sleep**: the ZyXEL Device is in power saving mode, but periodically checks whether a base station has traffic waiting. • **Idle**: the ZyXEL Device is in power saving mode, but can connect when a base station alerts it that there is traffic waiting. • **Handover**: the ZyXEL Device is moving from one coverage area to another, and is connecting to the new base station.
Bandwidth	This field shows the size of the bandwidth step the ZyXEL Device uses to connect to a base station in megahertz (MHz).
CINR mean	This field shows the average Carrier to Interference plus Noise Ratio of the current connection. This value is an indication of overall radio signal quality. A higher value indicates a higher signal quality, and a lower value indicates a lower signal quality.
CINR deviation	This field shows the amount of change in the CINR level. This value is an indication of radio signal stability. A lower number indicates a more stable signal, and a higher number indicates a less stable signal.
RSSI	This field shows the Received Signal Strength Indication. This value is a measurement of overall radio signal strength. A higher RSSI level indicates a stronger signal, and a lower RSSI level indicates a weaker signal.
UL Data Rate	This field shows the number of data packets uploaded from the ZyXEL Device to the base station each second.
DL Data Rate	This field shows the number of data packets downloaded to the ZyXEL Device from the base station each second.
PER	This field shows the Packet Error Rate. The PER is the percentage of data packets transmitted across the network but not successfully received.
Tx Power	This field shows the output transmission (Tx) level of the ZyXEL Device.
Site Information	Click this link to view details of the radio frequencies used by the ZyXEL Device to connect to a base station.
Profile	Click this link to view details of the current wireless security settings.

Table 6 Status Screen

LABEL	DESCRIPTION
System Status	
System Up Time	This field displays how long the ZyXEL Device has been running since it last started up. The ZyXEL Device starts up when you plug it in, when you restart it (**Maintenance > Tools > Restart**), or when you reset it (see Section 2.1.2 on page 35).
Current Date/ Time	This field displays the current date and time in the ZyXEL Device. You can change this in **Maintenance > System > Time Setting**.
CPU Usage	This field displays what percentage of the ZyXEL Device's processing ability is currently being used. The higher the CPU usage, the more likely the ZyXEL Device is to slow down. You can reduce this by disabling some services, such as DHCP, NAT, or content filtering.
Memory Usage	This field displays what percentage of the ZyXEL Device's memory is currently used. The higher the memory usage, the more likely the ZyXEL Device is to slow down. Some memory is required just to start the ZyXEL Device and to run the web configurator. You can reduce the memory usage by disabling some services (see **CPU Usage**); by reducing the amount of memory allocated to NAT and firewall rules (you may have to reduce the number of NAT rules or firewall rules to do so); or by deleting rules in functions such as incoming call policies, speed dial entries, and static routes.
IVR Usage	This field displays what percentage of the ZyXEL Device's IVR memory is currently used. IVR (Interactive Voice Response) refers to the customizable ring tone and on-hold music you set. See Section 10.1.11 on page 111 for more information.
Interface Status	
Interface	This column displays each interface of the ZyXEL Device.
Status	This field indicates whether or not the ZyXEL Device is using the interface. For the WAN interface, this field displays **Up** when the ZyXEL Device is connected to a WiMAX network, and **Down** when the ZyXEL Device is not connected to a WiMAX network. For the LAN interface, this field displays **Up** when the ZyXEL Device is using the interface and **Down** when the ZyXEL Device is not using the interface.
Rate	For the LAN ports this displays the port speed and duplex setting. For the WAN interface, it displays the downstream and upstream transmission rate or **N/A** if the ZyXEL Device is not connected to a base station.
Summary	
Any IP Table	Click this link to view a list of IP addresses and MAC addresses of computers connected to the ZyXEL Device but not in the same subnet.
Packet Statistics	Click this link to view port status and packet specific statistics.
DHCP Table	Click this link to see details of computers to which the ZyXEL Device has given an IP address.
VoIP Statistics	Click this link to view statistics about your VoIP usage.
VoIP Status	
Account	This column displays each SIP account in the ZyXEL Device.

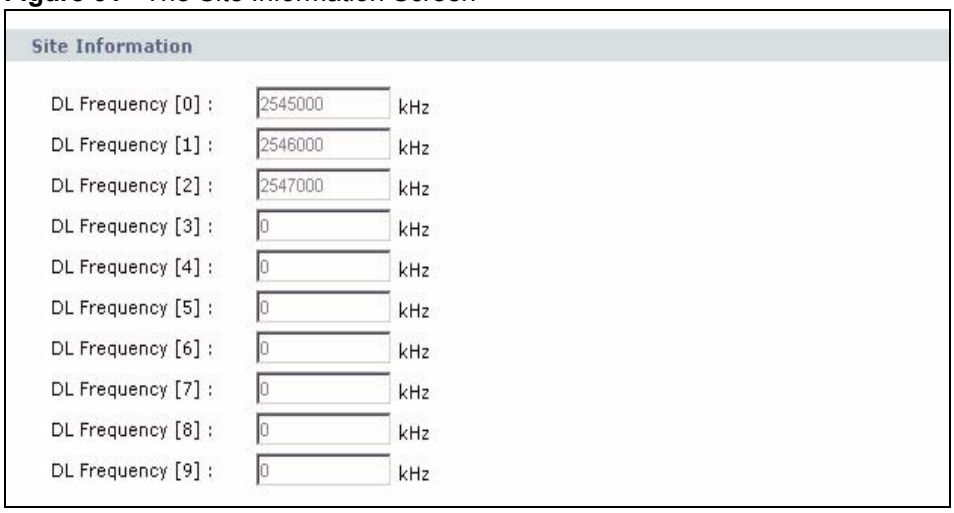
Table 6 Status Screen

LABEL	DESCRIPTION
Registration	This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP. If the SIP account is already registered with the SIP server, Click **Unregister** to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name. The second field displays **Registered**. If the SIP account is not registered with the SIP server, Click **Register** to have the ZyXEL Device attempt to register the SIP account with the SIP server. The second field displays the reason the account is not registered. **Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Settings**. **Register Fail** - The last time the ZyXEL Device tried to register the SIP account with the SIP server, the attempt failed. The ZyXEL Device automatically tries to register the SIP account when you turn on the ZyXEL Device or when you activate it.
URI	This field displays the account number and service domain of the SIP account. You can change these in **VoIP > SIP > SIP Settings**.

6.2 Site Information

Click **Status > Site Information** to view this screen. This read-only screen shows information about the ZyXEL Device's connection with a WiMAX base station. To configure these settings, go to the **Network > WAN > WiMAX Frequency** screen.

Figure 31 The Site Information Screen


Site Information
DL Frequency [0] : 2545000 kHz
DL Frequency [1] : 2546000 kHz
DL Frequency [2] : 2547000 kHz
DL Frequency [3] : 0 kHz
DL Frequency [4] : 0 kHz
DL Frequency [5] : 0 kHz
DL Frequency [6] : 0 kHz
DL Frequency [7] : 0 kHz
DL Frequency [8] : 0 kHz
DL Frequency [9] : 0 kHz

The following table describes the labels in this screen.

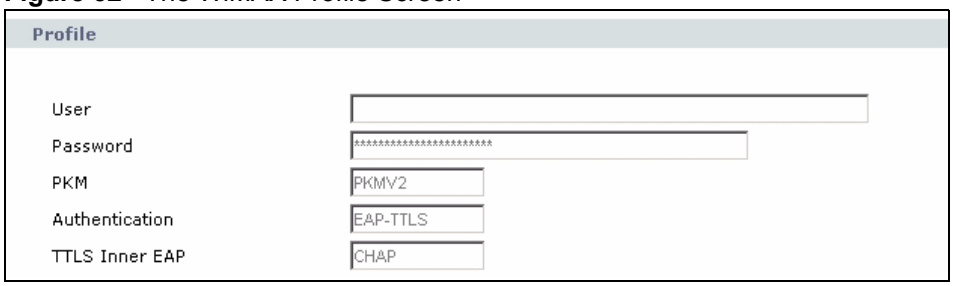
Table 7 The Site Information Screen

LABEL	DESCRIPTION
Site Information	
DL Frequency [0] ~ [9]	These fields show the downlink frequency settings in kilohertz (kHz). These settings determine how the ZyXEL Device searches for an available wireless connection. See Section 7.4 on page 74 for more information.

6.3 Profile

Click **Status > Profile** to view this screen. This read-only screen displays information about the security settings you are using. To configure these settings, go to the **Network > WAN > Internet Connection** screen.

Figure 32 The WiMAX Profile Screen



The following table describes the labels in this screen.

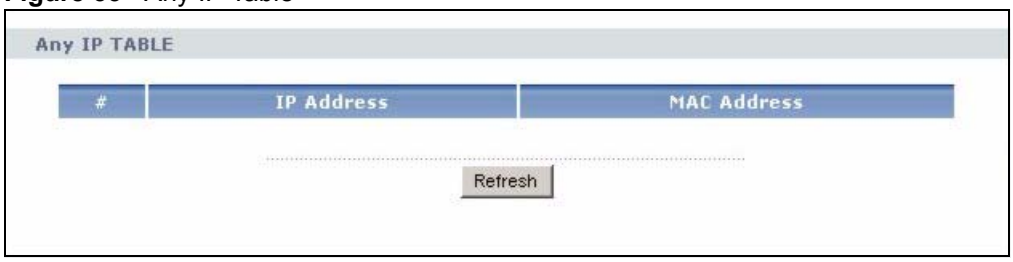
Table 8 The WiMAX Profile Screen

LABEL	DESCRIPTION
Profile	
User	This is the username for your Internet access account.
Password	This is the password for your Internet access account. The password displays as a row of asterisks.
PKM	This field displays the Privacy Key Management version number. PKM provides security between the ZyXEL Device and the base station. See the WiMAX security appendix for more information.
Authentication	This field displays the user authentication method. Authentication is the process of confirming the identity of a user (by means of a username and password, for example). EAP-TTLS allows an MS/SS and a base station to establish a secure link (or 'tunnel') with an AAA (Authentication, Authorization and Accounting) server in order to exchange authentication information. See the WiMAX security appendix for more details.
TTLS Inner EAP	This field displays the type of secondary authentication method. Once a secure EAP-TTLS connection is established, the inner EAP is the protocol used to exchange security information between the mobile station, the base station and the AAA server to authenticate the mobile station. At the time of writing, the ZyXEL Device supports only CHAP (Challenge Handshake Authentication Protocol). See the WiMAX security appendix for more details.

6.4 Any IP Table Window

This screen displays the IP address of each computer that is using the ZyXEL Device via the any IP feature. Any IP allows computers to access the Internet through the ZyXEL Device without changing their network settings when NAT is enabled. To access this screen, open the **Status** screen (see Section 6.1 on page 59), and click **(Details...)** next to **Any IP Table**.

Figure 33 Any IP Table



Each field is described in the following table.

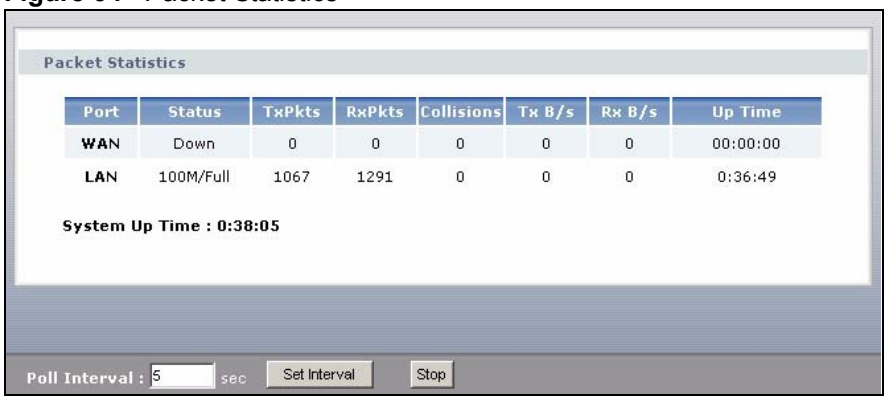
Table 9 Any IP Table

LABEL	DESCRIPTION
#	This field is a sequential value. It is not associated with a specific entry.
IP Address	This field displays the IP address of each computer that is using the ZyXEL Device but is in a different subnet than the ZyXEL Device.
MAC Address	This field displays the MAC address of the computer that is using the ZyXEL Device but is in a different subnet than the ZyXEL Device.
Refresh	Click this to update this screen.

6.5 Packet Statistics

To access this screen, open the **Status** screen (see Section 6.1 on page 59), and click **(Details...)** next to **Packet Statistics**. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

Figure 34 Packet Statistics



The following table describes the fields in this screen.

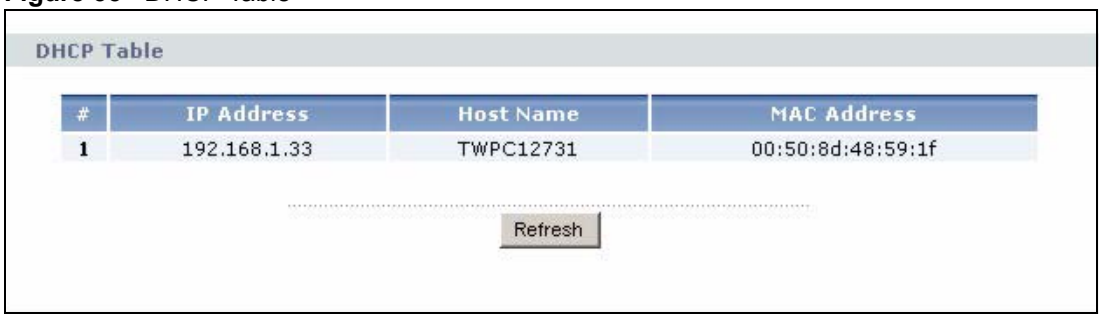
Table 10 Packet Statistics

LABEL	DESCRIPTION
Packet Statistics	
Port	This column displays each interface of the ZyXEL Device.
Status	This field indicates whether or not the ZyXEL Device is using the interface. For the WAN interface, this field displays **Up** when the ZyXEL Device is connected to a WiMAX network, and **Down** when the ZyXEL Device is not connected to a WiMAX network. For the LAN interface, this field displays **Up** when the ZyXEL Device is using the interface and **Down** when the ZyXEL Device is not using the interface.
TxPkts	This field displays the number of packets transmitted on this interface.
RxPkts	This field displays the number of packets received on this interface.
Collisions	This field displays the number of collisions on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this interface has been connected.
System up Time	This is the elapsed time the system has been on.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval** field above.
Stop	Click this button to halt the refreshing of the system statistics.

6.6 DHCP Table Screen

This screen displays information about computers that received an IP address from the ZyXEL Device. To access this screen, open the **Status** screen (see Section 6.1 on page 59), and click **(Details...)** next to **DHCP Table**.

Figure 35 DHCP Table



Each field is described in the following table.

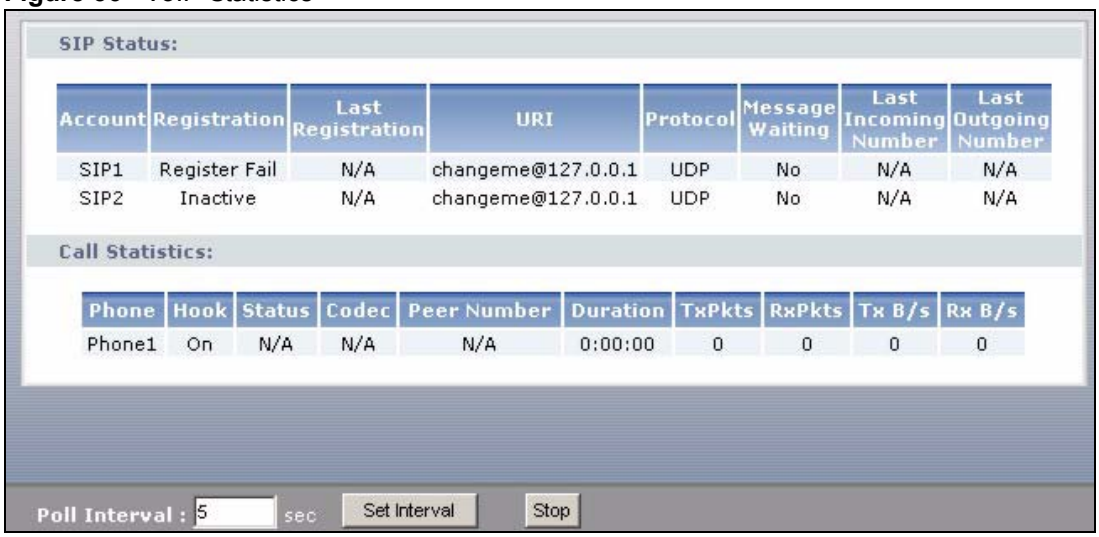
Table 11 DHCP Table

LABEL	DESCRIPTION
DHCP Table	
#	This field is a sequential value. It is not associated with a specific entry.
IP Address	This field displays the IP address the ZyXEL Device assigned to a computer in the network.
Host Name	This field displays the system name of the computer to which the ZyXEL Device assigned the IP address.
MAC Address	This field displays the MAC address of the computer to which the ZyXEL Device assigned the IP address.
Refresh	Click this to update this screen.

6.7 VoIP Statistics Window

This screen displays SIP registration information, status of calls and VoIP traffic statistics. To access this screen, open the **Status** screen (see Section 6.1 on page 59), and click **(Details...)** next to **VoIP Statistics**.

Figure 36 VoIP Statistics



Each field is described in the following table.

Table 12 VoIP Statistics

LABEL	DESCRIPTION
SIP Status	
Account	This column displays each SIP account in the ZyXEL Device.
Registration	This field displays the current registration status of the SIP account. You can change this in the **Status** screen. **Registered** - The SIP account is registered with a SIP server. **Register Fail** - The last time the ZyXEL Device tried to register the SIP account with the SIP server, the attempt failed. The ZyXEL Device automatically tries to register the SIP account when you turn on the ZyXEL Device or when you activate it. **Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Settings**.
Last Registration	This field displays the last time you successfully registered the SIP account. It displays **N/A** if you never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in **VoIP > SIP > SIP Settings**.
Protocol	This field displays the transport protocol the SIP account uses. SIP accounts always use UDP.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. It displays **N/A** if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. It displays **N/A** if the SIP account has never dialed a number.
Call Statistics	
Phone	This field displays the ZyXEL Device's phone port number.

Table 12 VoIP Statistics

LABEL	DESCRIPTION
Hook	This field indicates whether the phone is on the hook or off the hook. **On** - The phone is hanging up or already hung up. **Off** - The phone is dialing, calling, or connected.
Status	This field displays the current state of the phone call. **N/A** - There are no current VoIP calls, incoming calls or outgoing calls being made. **DIAL** - The callee's phone is ringing. **RING** - The phone is ringing for an incoming VoIP call. **Process** - There is a VoIP call in progress. **DISC** - The callee's line is busy, the callee hung up or your phone was left off the hook.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Duration	This field displays how long the current call has lasted.
Tx Pkts	This field displays the number of packets the ZyXEL Device has transmitted in the current call.
Rx Pkts	This field displays the number of packets the ZyXEL Device has received in the current call.
Tx B/s	This field displays how quickly the ZyXEL Device has transmitted packets in the current call. The rate is the average number of bytes transmitted per second.
Rx B/s	This field displays how quickly the ZyXEL Device has received packets in the current call. The rate is the average number of bytes transmitted per second.
Poll Interval(s)	Enter how often you want the ZyXEL Device to update this screen, and click **Set Interval**.
Set Interval	Click this to make the ZyXEL Device update the screen based on the amount of time you specified in **Poll Interval**.
Stop	Click this to make the ZyXEL Device stop updating the screen.

CHAPTER 7
WAN Setup

This chapter describes how to configure WAN settings.

7.1 WAN Overview

A WAN (Wide Area Network) is an outside connection to another network or the Internet. Your ZyXEL Device uses the IEEE 802.16e WiMAX standard to connect wirelessly to a WiMAX base station (see Section 1.1 on page 29).

7.2 WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) is the IEEE 802.16 wireless networking standard, which provides high-bandwidth, wide-range wireless service across wireless Metropolitan Area Networks (MANs). ZyXEL is a member of the WiMAX Forum, the industry group dedicated to promoting and certifying interoperability of wireless broadband products.

In a wireless MAN, a wireless-equipped computer is known either as a mobile station (MS) or a subscriber station (SS). Mobile stations use the IEEE 802.16e standard and are able to maintain connectivity while switching their connection from one base station to another base station (handover) while subscriber stations use other standards that do not have this capability (IEEE 802.16-2004, for example). The following figure shows an MS-equipped notebook computer **MS1** moving from base station **BS1**'s coverage area and connecting to **BS2**.

Figure 37 WiMax: Mobile Station

WiMAX technology uses radio signals (around 2 to 10 GHz) to connect subscriber stations and mobile stations to local base stations. Numerous subscriber stations and mobile stations connect to the network through a single base station (BS), as in the following figure.

Figure 38 WiMAX: Multiple Mobile Stations

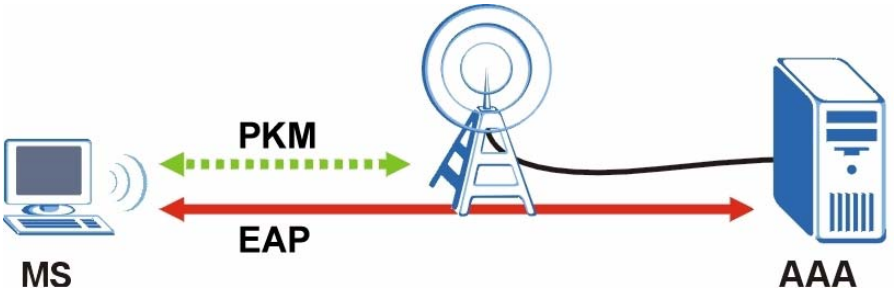
A base station's coverage area can extend over many hundreds of meters, even under poor conditions. A base station provides network access to subscriber stations and mobile stations, and communicates with other base stations.

7.2.1 Authentication

When authenticating a user, the base station uses a third-party RADIUS or Diameter server known as an AAA (Authentication, Authorization and Accounting) server to authenticate the mobile or subscriber stations.

The following figure shows a base station using an **AAA** server to authenticate mobile station **MS**, allowing it to access the Internet.

Figure 39 Using an AAA Server

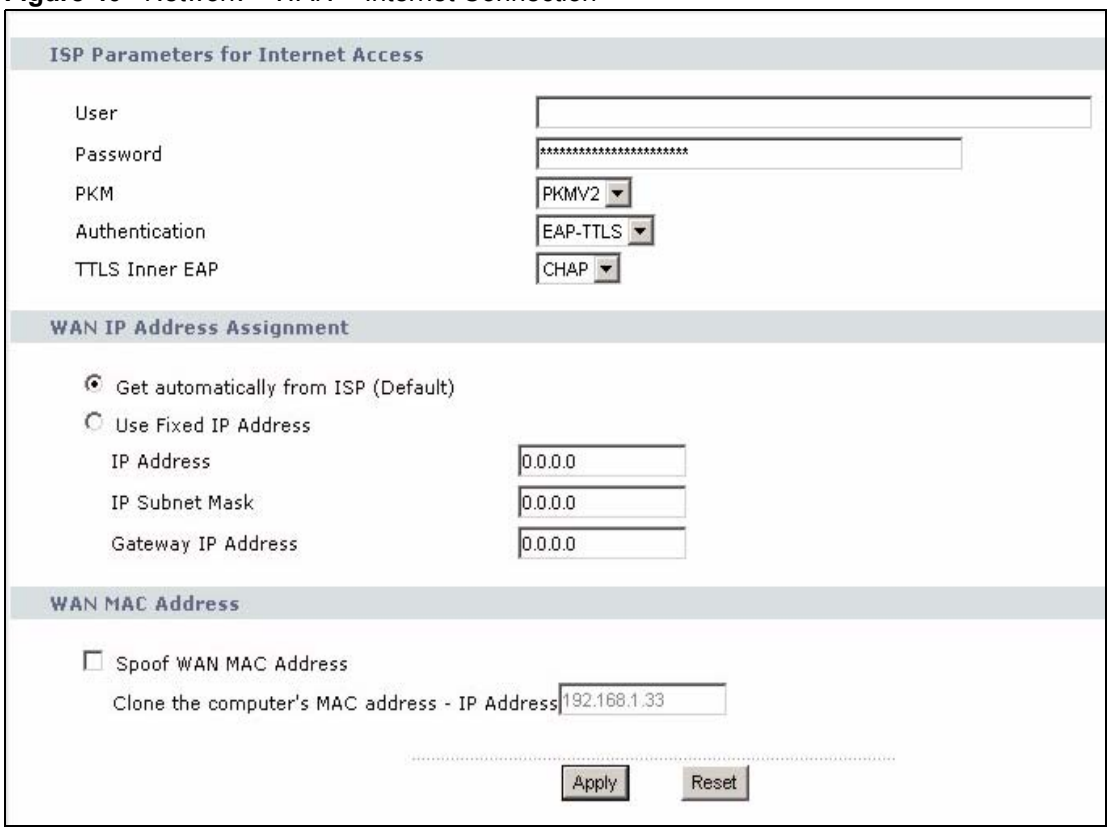


In this figure, the dashed arrow shows the PKM (Privacy Key Management) secured connection between the mobile station and the base station, and the solid arrow shows the EAP secured connection between the mobile station, the base station and the AAA server. See the WiMAX security appendix for more details.

7.3 Internet Access Setup

To change your ZyXEL Device's Internet access settings, click **Network > WAN**. The **Internet Connection** screen displays.

Figure 40 Network > WAN > Internet Connection



The following table describes the labels in this screen.

Table 13 Network > WAN > Internet Connection

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
User	Use this field to enter the username associated with your Internet access account. You can enter up to 61 printable ASCII characters.
Password	Use this field to enter the password associated with your Internet access account. You can enter up to 47 printable ASCII characters.
PKM	This field displays the Privacy Key Management version number. PKM provides security between the ZyXEL Device and the base station. At the time of writing, the ZyXEL Device supports PKMv2 only. See the WiMAX security appendix for more information.
Authentication	This field displays the user authentication method. Authentication is the process of confirming the identity of a mobile station (by means of a username and password, for example). At the time of writing, the ZyXEL Device supports EAP-TTLS only. EAP-TTLS allows a mobile station and a base station to establish a secure link with an AAA (Authentication, Authorization and Accounting) server in order to exchange authentication information. See the WiMAX security appendix for more details.

Table 13 Network > WAN > Internet Connection

LABEL	DESCRIPTION
TTLS Inner EAP	This field displays the type of secondary authentication method. Once a secure EAP-TTLS connection is established, the inner EAP is the protocol used to exchange security information between the mobile station, the base station and the AAA server to authenticate the mobile station. At the time of writing, the ZyXEL Device supports only CHAP (Challenge Handshake Authentication Protocol). See the WiMAX security appendix for more details.
WAN IP Address Assignment	
Get automatically from ISP (Default)	Select this if you have a dynamic IP address. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.
Use Fixed IP Address	A static IP address is a fixed IP that your ISP gives you. Type your ISP assigned IP address in the **IP Address** field below.
IP Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendices to calculate a subnet mask If you are implementing subnetting.
Gateway IP Address	Specify a gateway IP address (supplied by your ISP).
WAN MAC Address	
Spoof WAN MAC Address	You can use the factory-assigned default MAC Address, or clone the MAC address of a computer or other network device on your LAN. To clone a MAC address, select the check box next to **Spoof WAN MAC Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file. Otherwise, configure nothing to have the ZyXEL Device use the factory-assigned default MAC address.
Clone the computer's MAC address - IP address:	Enter the IP address of the computer on the LAN whose MAC you are cloning. It is recommended that you clone the MAC address prior to hooking up the WAN port.
Apply	Click this button to save your settings.
Reset	Click this button to return all the fields in this screen to their default values.

7.4 Frequency Settings

In a WiMAX network, a mobile or subscriber station must use a radio frequency supported by the base station to communicate. When the ZyXEL Device looks for a connection to a base station, it can search a range of frequencies.

Radio frequency is measured in Hertz (Hz).

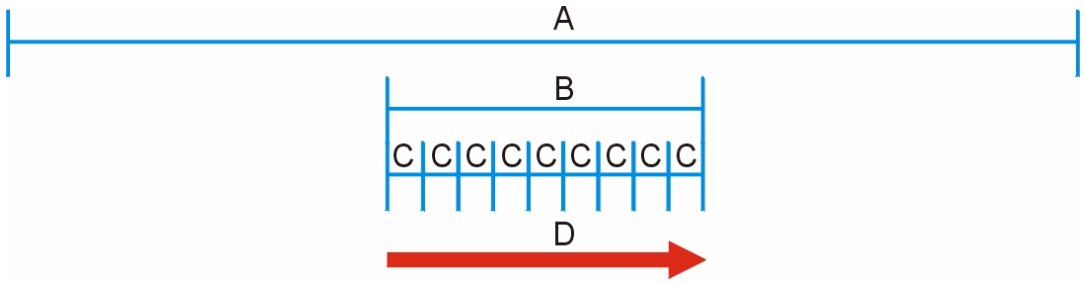
Table 14 Radio Frequency Conversion

1 kHz = 1000 Hz
1 MHz = 1000 kHz (1000000 Hz)
1 GHz = 1000 MHz (1000000 kHz)

7.4.1 Frequency Ranges

The following figure shows the ZyXEL Device searching a range of frequencies to find a connection to a base station.

Figure 41 Frequency Ranges



In this figure, **A** is the WiMAX frequency range. "WiMAX frequency range" refers to the entire range of frequencies the ZyXEL Device is capable of using to transmit and receive (see the Product Specifications appendix for details).

In the figure, **B** shows the operator frequency range. This is the range of frequencies within the WiMAX frequency range supported by your operator (service provider).

The operator range is subdivided into bandwidth steps. In the figure, each **C** is a bandwidth step.

The arrow **D** shows the ZyXEL Device searching for a connection.

Have the ZyXEL Device search only certain frequencies by configuring the downlink frequencies. Your operator can give you information on the supported frequencies.

The downlink frequencies are points of the frequency range your ZyXEL Device searches for an available connection. Use the **Site Survey** screen to set these bands. You can set the downlink frequencies anywhere within the WiMAX frequency range. In this example, the downlink frequencies have been set to search all of the operator range for a connection.

7.4.2 Configuring Frequency Settings

You need to set the ZyXEL Device to scan one or more specific radio frequencies to find an available connection to a WiMAX base station.

Use the **WiMAX Frequency** screen to define the radio frequencies to be searched for available wireless connections. See Section 7.4.2.1 on page 77 for an example of using the **WiMAX Frequency** screen.

- The ZyXEL Device searches the **DL Frequency** settings in ascending numerical order, from **[0]** to **[9]**.
- If you enter a 0 in a **DL Frequency** field, the ZyXEL Device immediately moves on to the next **DL Frequency** field.
- When the ZyXEL Device connects to a base station, the values in this screen are automatically set to the base station's frequency. The next time the ZyXEL Device searches for a connection, it searches only this frequency. If you want the ZyXEL Device to search other frequencies, enter them in the **DL Frequency** fields.

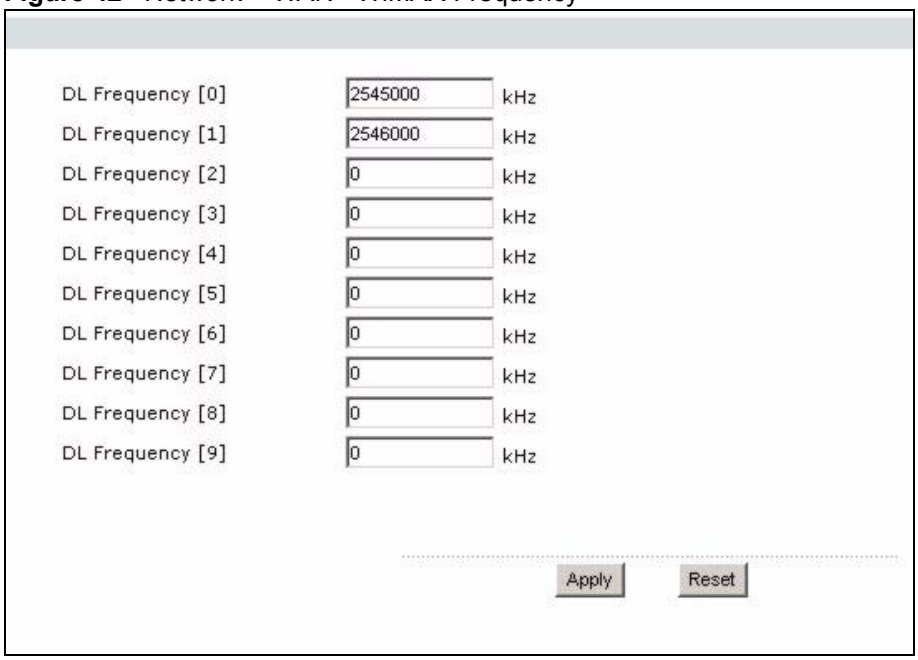
The following table describes some examples of **DL Frequency** settings.

Table 15 DL Frequency Example Settings

	EXAMPLE 1	EXAMPLE 2
DL Frequency [0]:	2500000	2500000
DL Frequency [1]:	2550000	2550000
DL Frequency [2]	0	2600000
DL Frequency [3]:	0	0
DL Frequency [4]:	0	0
	The ZyXEL Device searches at 2500000 kHz, and then searches at 2550000 kHz if it has not found a connection.	The ZyXEL Device searches at 2500000 kHz and then at 2550000 kHz if it has not found an available connection. If it still does not find an available connection, it searches at 2600000 kHz.

Click **Network > WAN > WiMAX Frequency** to display the screen shown next.

Figure 42 Network > WAN >WiMAX Frequency



The following table describes the labels in this screen.

Table 16 Network > WAN > WiMAX Frequency

LABEL	DESCRIPTION
DL Frequency [0] ~ [9]	These fields show the downlink frequency settings in kilohertz (kHz). Enter values in these fields to have the ZyXEL Device scan these frequencies for available channels in ascending numerical order. Contact your service provider for details of supported frequencies.
Apply	Click this button to save your settings.
Reset	Click this button to return all the fields in this screen to their default values.

7.4.2.1 Using the WiMAX Frequency Screen: Example

In this example, your Internet service provider has given you a list of supported frequencies, as follows.

Table 17 Example Supported Frequencies (GHz)

2.5
2.525
2.6
2.625

Use the **WiMAX Frequency** screen to enter the frequencies you want the ZyXEL Device to scan for a connection to a base station.

1 In the **DL Frequency [0]** field, enter **2500000** (2500000 kilohertz (kHz) is equal to 2.5 gigahertz).

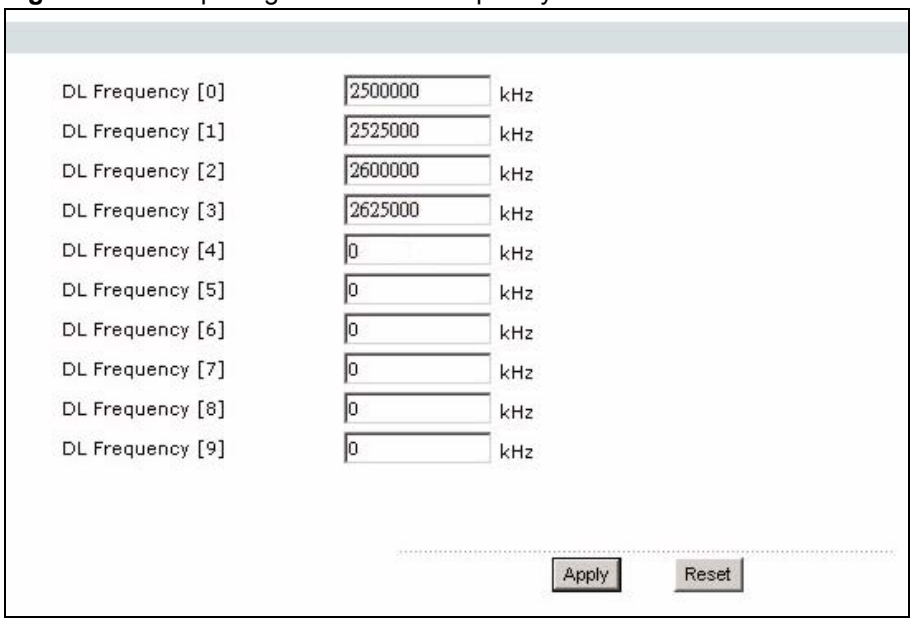
2 In the **DL Frequency [1]** field, enter **2525000**.

3 In the **DL Frequency [2]** field, enter **2600000**.

4 In the **DL Frequency [3]** field, enter **2625000**.

Leave the rest of the **DL Frequency** fields at zero. The screen appears as follows.

Figure 43 Completing the WiMAX Frequency Screen


DL Frequency [0] 2500000 kHz
DL Frequency [1] 2525000 kHz
DL Frequency [2] 2600000 kHz
DL Frequency [3] 2625000 kHz
DL Frequency [4] 0 kHz
DL Frequency [5] 0 kHz
DL Frequency [6] 0 kHz
DL Frequency [7] 0 kHz
DL Frequency [8] 0 kHz
DL Frequency [9] 0 kHz
Apply
Reset

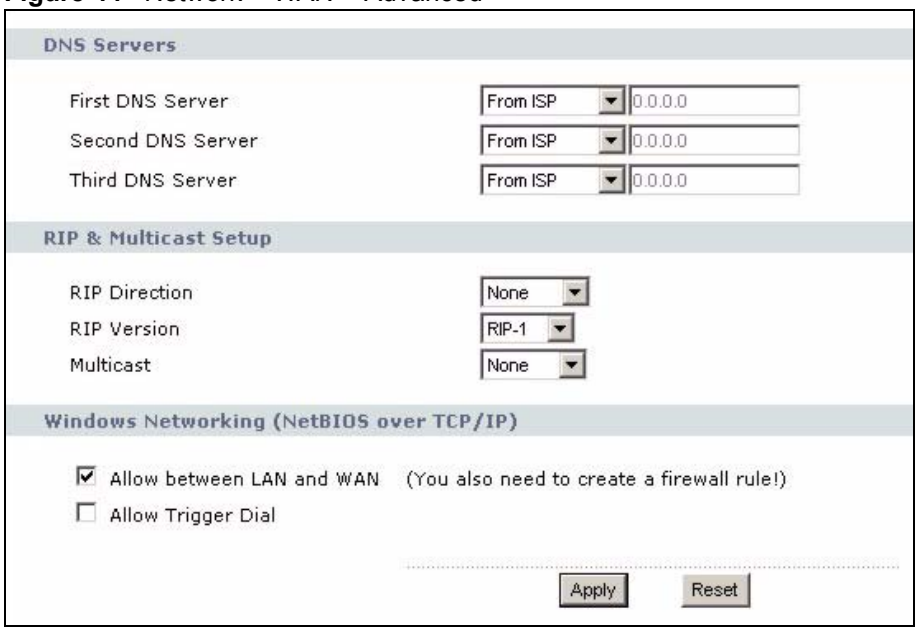
5 Click **Apply**. The ZyXEL Device stores your settings.

When the ZyXEL Device searches for available frequencies, it scans all frequencies from **DL Frequency [0]** to **DL Frequency [3]**. When it finds an available connection, the fields in this screen will be automatically set to use that frequency.

7.5 Configuring Advanced WAN Settings

Click **Network > WAN > Advanced** to display the following screen.

Figure 44 Network > WAN > Advanced



The following table describes the labels in this screen.

Table 18 Network > WAN > Advanced

LABEL	DESCRIPTION
DNS Servers	
First, Second and Third DNS Server	Select **Obtained from ISP** if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). Use the drop-down list box to select a DNS server IP address that the ISP assigns in the field to the right. Select **UserDefined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **UserDefined**, but leave the IP address set to 0.0.0.0, **UserDefined** changes to **None** after you click **Apply**. If you set a second choice to **UserDefined**, and enter the same IP address, the second **UserDefined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**.
RIP Version	Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**. Select **None** to disable it.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.

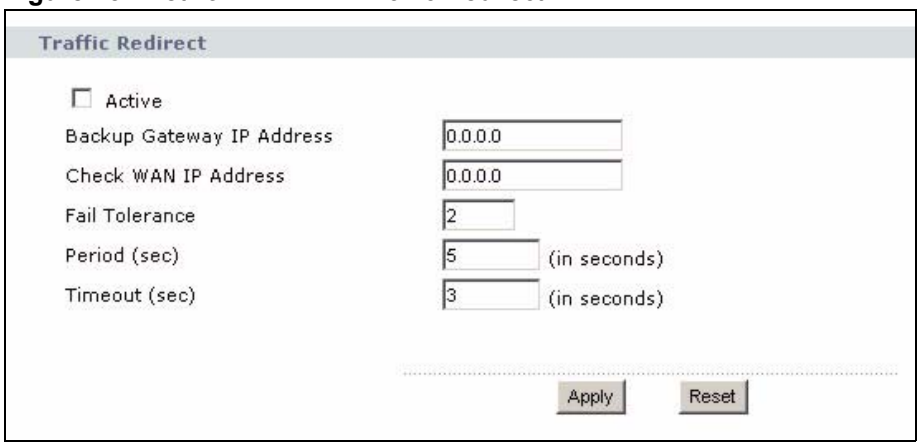
Table 18 Network > WAN > Advanced

LABEL	DESCRIPTION
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click this button to save your settings.
Reset	Click this button to return all the fields in this screen to their default values.

7.6 Configuring Traffic Redirect Settings

To change your ZyXEL Device's traffic redirect settings, click **Network > WAN > Traffic Redirect**. The screen appears as shown.

Figure 45 Network > WAN > Traffic Redirect



The following table describes the labels in this screen.

Table 19 Network > WAN > Traffic Redirect

LABEL	DESCRIPTION
Traffic Redirect	
Active	Select this check box to have the ZyXEL Device use traffic redirect if the normal WAN connection goes down. **Note:** If you activate traffic redirect, you must configure the **Check WAN IP Address** field.
Backup Gateway IP Address	Type the IP address of your backup gateway in dotted decimal notation. The ZyXEL Device automatically forwards traffic to this IP address if the ZyXEL Device's Internet connection terminates.

Table 19 Network > WAN > Traffic Redirect

LABEL	DESCRIPTION
Check WAN IP Address	Configure this field to test your ZyXEL Device's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). **Note:** If you activate either traffic redirect or dial backup, you must configure an IP address here. When using a WAN backup connection, the ZyXEL Device periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
Fail Tolerance	Type the number of times (2 recommended) that your ZyXEL Device may ping the IP addresses configured in the **Check WAN IP Address** field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Period (sec)	The ZyXEL Device tests a WAN connection by periodically sending a ping to either the default gateway or the address in the **Check WAN IP Address** field. Type a number of seconds (5 to 300) to set the time interval between checks. Allow more time if your destination IP address handles lots of traffic.
Timeout (sec)	Type the number of seconds (1 to 10) for your ZyXEL Device to wait for a response to the ping before considering the check to have failed. This setting must be less than the **Period**. Use a higher value in this field if your network is busy or congested.
Apply	Click this button to save your settings.
Reset	Click this button to return all the fields in this screen to their default values.

CHAPTER 8
LAN

Use these screens to set up the ZyXEL Device on the LAN. You can configure its IP address and subnet mask, DHCP services, and other subnets. You can also control how the ZyXEL Device sends routing information using RIP, and you can enable and disable Any IP.

8.1 LAN Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is usually a computer network limited to the immediate area, such as the same building or floor of a building.

8.1.1 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyXEL Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your ZyXEL Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

8.1.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else each computer must be manually configured.

The ZyXEL Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), see Section 8.2.2 on page 88.

8.1.3 LAN TCP/IP

The ZyXEL Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

The LAN parameters of the ZyXEL Device are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), see Section 8.2.2 on page 88.

8.1.4 DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If your ISP gives you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**, otherwise, leave them blank.

Some ISPs choose to pass the DNS servers using the DNS server extensions of PPP IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The ZyXEL Device supports the IPCP DNS server extensions through the DNS proxy feature.

If the **Primary** and **Secondary DNS Server** fields in the **LAN Setup** screen are not specified, for instance, left as 0.0.0.0, the ZyXEL Device tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **LAN Setup** screen. This way, the ZyXEL Device can pass the DNS servers to the computers and the computers can query the DNS server directly without the ZyXEL Device's intervention.

8.1.5 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both -** the ZyXEL Device will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only -** the ZyXEL Device will not send any RIP packets but will accept all RIP packets received.
- **Out Only -** the ZyXEL Device will send out RIP packets but will not accept any RIP packets received.
- **None -** the ZyXEL Device will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

8.1.6 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address

224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information. IP multicasting can be enabled/disabled on the ZyXEL Device LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

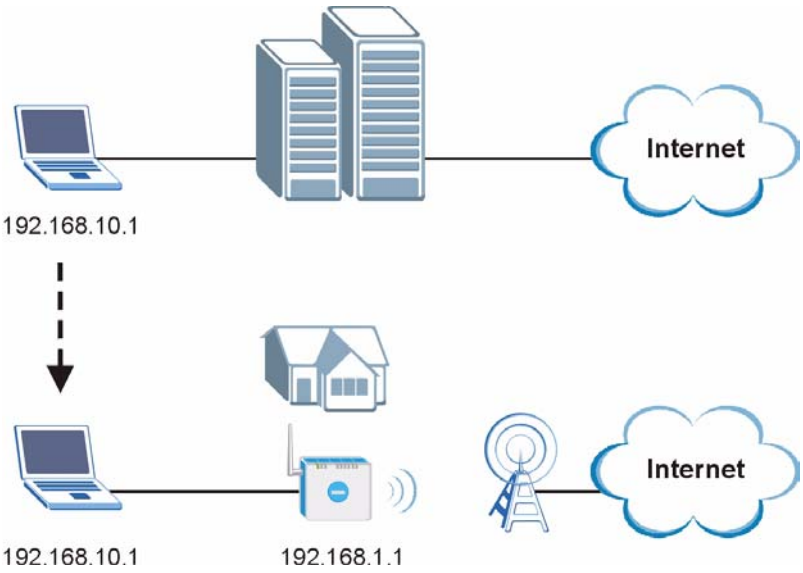
8.1.7 Any IP

Traditionally, you must set the IP addresses and the subnet masks of a computer and the ZyXEL Device to be in the same subnet to allow the computer to access the Internet (through the ZyXEL Device). In cases where your computer is required to use a static IP address in another network, you may need to manually configure the network settings of the computer every time you want to access the Internet via the ZyXEL Device.

With the Any IP feature and NAT enabled, the ZyXEL Device allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the ZyXEL Device are not in the same subnet. Whether a computer is set to use a dynamic or static (fixed) IP address, you can simply connect the computer to the ZyXEL Device and access the Internet.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a ZyXEL Device is installed, you can still use the computer to access the Internet without changing the network settings, even when the IP addresses of the computer and the ZyXEL Device are not in the same subnet.

Figure 46 Any IP Example



The Any IP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the ZyXEL Device's IP address.

Note: You *must* enable NAT to use the Any IP feature on the ZyXEL Device.

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network. IP routing table is defined on IP Ethernet devices (the ZyXEL Device) to decide which hop to use, to help forward data along to its specified destination.

The following lists out the steps taken, when a computer tries to access the Internet for the first time through the ZyXEL Device.

1. When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the ZyXEL Device) by looking at the MAC address in its ARP table.
2. When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.
3. The ZyXEL Device receives the ARP request and replies to the computer with its own MAC address.
4. The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the ZyXEL Device.
5. When the ZyXEL Device receives packets from the computer, it creates an entry in the IP routing table so it can properly forward packets intended for the computer.

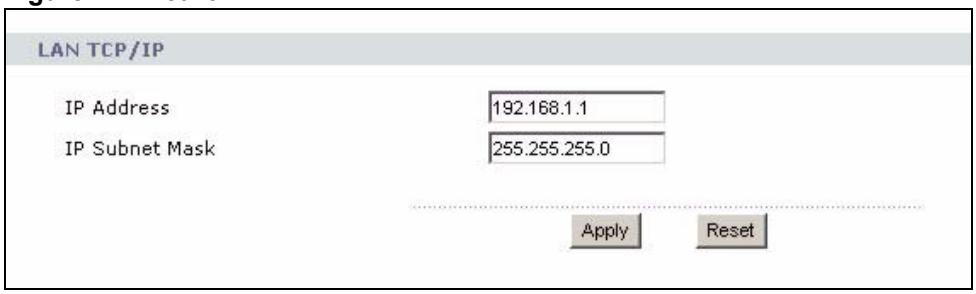
After all the routing information is updated, the computer can access the ZyXEL Device and the Internet as if it is in the same subnet as the ZyXEL Device.

8.2 LAN Screens

8.2.1 LAN IP Screen

Use this screen to set up the ZyXEL Device's IP address and subnet mask. To access this screen, click **Network > LAN > IP**.

Figure 47 Network > LAN > IP



Each field is described in the following table.

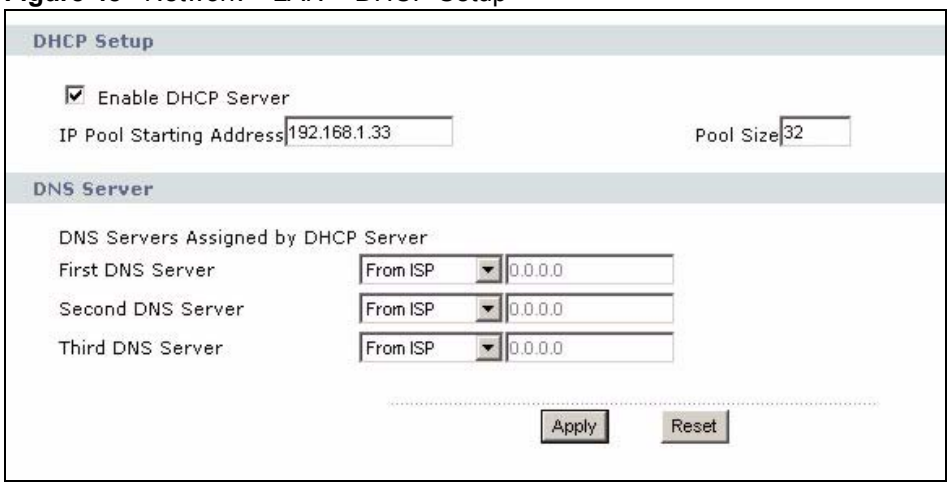
Table 20 Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Enter the IP address of the ZyXEL Device on the LAN. **Note:** This field is the IP address you use to access the ZyXEL Device on the LAN. If the web configurator is running on a computer on the LAN, you lose access to the web configurator as soon as you change this field and click **Apply**. You can access the web configurator again by typing the new IP address in the browser.
IP Subnet Mask	Enter the subnet mask of the LAN.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its default value.

8.2.2 LAN DHCP Setup Screen

Use this screen to enable, disable, and configure the DHCP server in the ZyXEL Device. To access this screen, click **Network > LAN > DHCP Setup**.

Figure 48 Network > LAN > DHCP Setup



Each field is described in the following table.

Table 21 Network > LAN > DHCP Setup

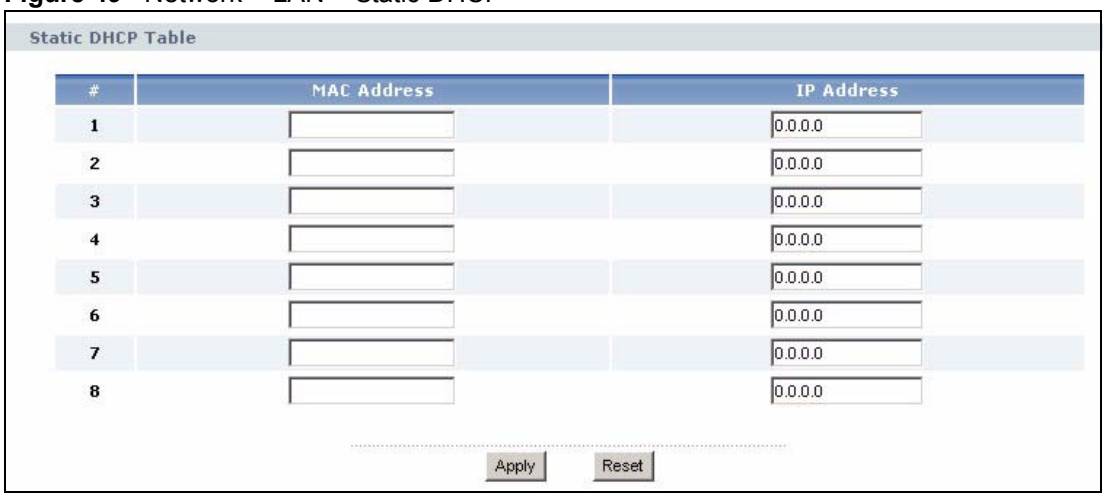
LABEL	DESCRIPTION
DHCP Setup	
Enable DHCP Server	Select this if you want the ZyXEL Device to be the DHCP server on the LAN. As a DHCP server, the ZyXEL Device assigns IP addresses to DHCP clients on the LAN and provides the subnet mask and DNS server information.
IP Pool Starting Address	Enter the IP address from which the ZyXEL Device begins allocating IP addresses, if you have not specified an IP address for this computer in **Network > LAN > Static DHCP**.
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by a subnet mask of 255.255.255.0 (regardless of the subnet the ZyXEL Device is in). For example, if the **IP Pool Start Address** is 10.10.10.10, the ZyXEL Device can allocate up to 10.10.10.254, or 245 IP addresses.
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses of a maximum of three DNS servers that the network can use. The ZyXEL Device provides these IP addresses to DHCP clients. You can specify these IP addresses two ways. **From ISP** - provide the DNS servers provided by the ISP on the WAN port. **User Defined** - enter a static IP address. **DNS Relay** - this setting will relay DNS information from the DNS server obtained by the ZyXEL Device. **None** - no DNS service will be provided by the ZyXEL Device.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its default value.

8.2.3 LAN Static DHCP Screen

Note: This screen has no effect if the DHCP server is not enabled. You can enable it in **Network > LAN > DHCP Setup**.

Use this screen to make the ZyXEL Device assign a specific IP address to a specific computer on the LAN. To access this screen, click **Network > LAN > Static DHCP**.

Figure 49 Network > LAN > Static DHCP



Each field is described in the following table.

Table 22 Network > LAN > Static DHCP

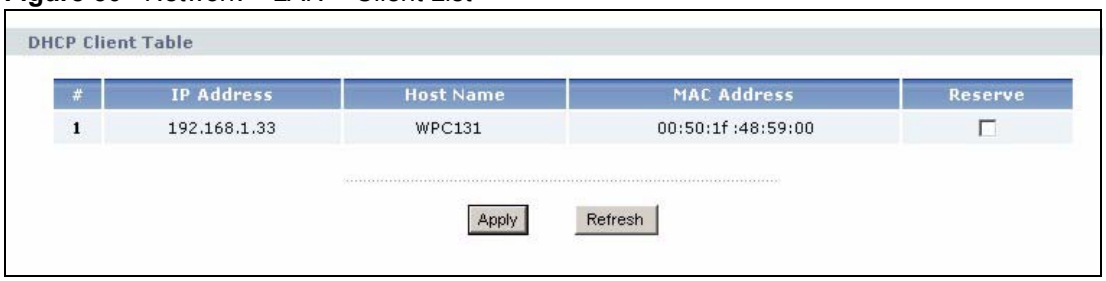
LABEL	DESCRIPTION
#	This field is a sequential value. It is not associated with a specific entry.
MAC Address	Enter the MAC address of the computer to which you want the ZyXEL Device to assign the same IP address.
IP Address	Enter the IP address you want the ZyXEL Device to assign to the computer.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its default value.

8.2.4 LAN Client List Screen

Note: This screen is empty if the DHCP server is not enabled. You can enable it in **Network > LAN > DHCP Setup**.

Use this screen to look at the IP addresses the ZyXEL Device has assigned to DHCP clients on the LAN. To access this screen, click **Network > LAN > Client List**.

Figure 50 Network > LAN > Client List



Each field is described in the following table.

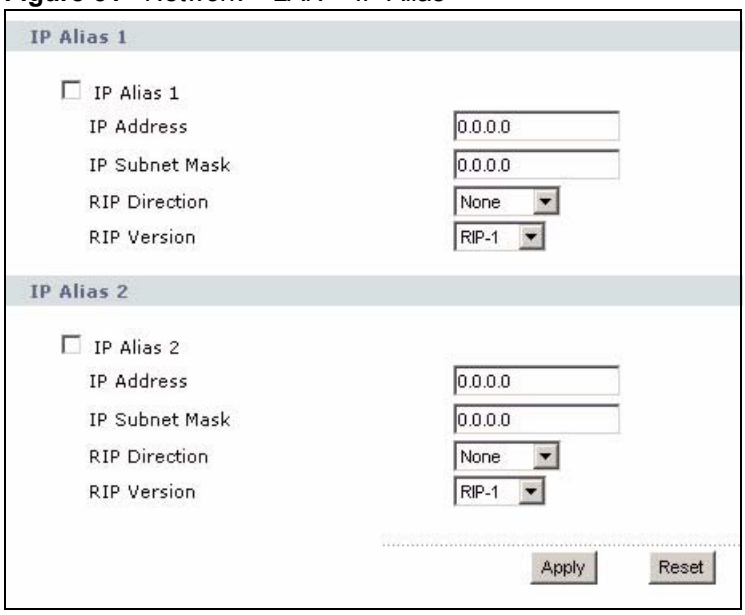
Table 23 Network > LAN > Client List

LABEL	DESCRIPTION
#	This field is a sequential value. It is not associated with a specific entry.
IP Address	This field displays the IP address the ZyXEL Device assigned to the computer.
Host Name	This field displays the system name of the computer to which the ZyXEL Device assigned the IP address.
MAC Address	This field displays the MAC address of the computer to which the ZyXEL Device assigned the IP address.
Reserve	Select this if you want to always assign this IP address to this MAC address. Then, click **Apply**. The ZyXEL Device creates an entry in the **LAN Static DHCP** screen. See Section 8.2.2 on page 88.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its default value.

8.2.5 LAN IP Alias Screen

Use this screen to add subnets on the LAN port. You can also control what routing information is sent and received by each subnet. To access this screen, click **Network > LAN > IP Alias**.

Figure 51 Network > LAN > IP Alias



Each field is described in the following table.

Table 24 Network > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias 1	
IP Alias 1	Select this to add the specified subnet to the LAN port.
IP Address	Enter the IP address of the ZyXEL Device on the subnet.
IP Subnet Mask	Enter the subnet mask of the subnet.
RIP Direction	Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. **None** - The ZyXEL Device does not send or receive routing information on the subnet. **Both** - The ZyXEL Device sends and receives routing information on the subnet. **In Only** - The ZyXEL Device only receives routing information on the subnet. **Out Only** - The ZyXEL Device only sends routing information on the subnet.
RIP Version	Select which version of RIP the ZyXEL Device uses when it sends or receives information on the subnet. **RIP-1** - The ZyXEL Device uses RIPv1 to exchange routing information. **RIP-2B** - The ZyXEL Device broadcasts RIPv2 to exchange routing information. **RIP-2M** - The ZyXEL Device multicasts RIPv2 to exchange routing information.
IP Alias 2	
IP Alias 2	Select this to add the specified subnet to the LAN port.
IP Address	Enter the IP address of the ZyXEL Device on the subnet.
IP Subnet Mask	Enter the subnet mask of the subnet.

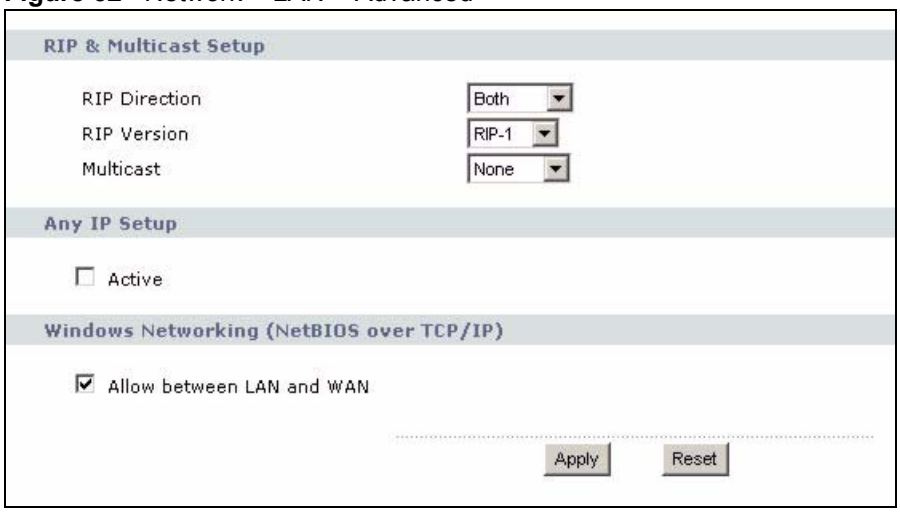
Table 24 Network > LAN > IP Alias

LABEL	DESCRIPTION
RIP Direction	Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. **None** - The ZyXEL Device does not send or receive routing information on the subnet. **Both** - The ZyXEL Device sends and receives routing information on the subnet. **In Only** - The ZyXEL Device only receives routing information on the subnet. **Out Only** - The ZyXEL Device only sends routing information on the subnet.
RIP Version	Select which version of RIP the ZyXEL Device uses when it sends or receives information on the subnet. **RIP-1** - The ZyXEL Device uses RIPv1 to exchange routing information. **RIP-2B** - The ZyXEL Device broadcasts RIPv2 to exchange routing information. **RIP-2M** - The ZyXEL Device multicasts RIPv2 to exchange routing information.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its default value.

8.2.6 LAN Advanced Screen

Use this screen to activate or deactivate the Any IP feature. You can also control what routing information is sent and received by each subnet. To access this screen, click **Network > LAN > Advanced**.

Figure 52 Network > LAN > Advanced



Each field is described in the following table.

Table 25 Network > LAN > Advanced

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. **None** - The ZyXEL Device does not send or receive routing information on the subnet. **Both** - The ZyXEL Device sends and receives routing information on the subnet. **In Only** - The ZyXEL Device only receives routing information on the subnet. **Out Only** - The ZyXEL Device only sends routing information on the subnet.
RIP Version	Select which version of RIP the ZyXEL Device uses when it sends or receives information on the subnet. **RIP-1** - The ZyXEL Device uses RIPv1 to exchange routing information. **RIP-2B** - The ZyXEL Device broadcasts RIPv2 to exchange routing information. **RIP-2M** - The ZyXEL Device multicasts RIPv2 to exchange routing information.
Multicast	You do not have to enable multicasting to use **RIP-2M**. (See **RIP Version**.) Select which version of IGMP the ZyXEL Device uses to support multicasting on the LAN. Multicasting sends packets to some computers on the LAN and is an alternative to unicasting (sending packets to one computer) and broadcasting (sending packets to every computer). **None** - The ZyXEL Device does not support multicasting. **IGMP-v1** - The ZyXEL Device supports IGMP version 1. **IGMP-v2** - The ZyXEL Device supports IGMP version 2. Multicasting can improve overall network performance. However, it requires extra processing and generates more network traffic. In addition, other computers on the LAN have to support the same version of IGMP.
Any IP Setup	
Active	Select this if you want to let computers on different subnets use the ZyXEL Device.
Windows Networking	NetBIOS over TCP/IP

Table 25 Network > LAN > Advanced

LABEL	DESCRIPTION
Allow between LAN and WAN	Select this check box if you want the ZyXEL Device to send NetBIOS (Network Basic Input/Output System) packets between the LAN and WAN. You should also make sure that NetBIOS packets are not blocked in **Security > Firewall > Services**. NetBIOS packets are TCP or UDP packets that enable a computer to connect to and communicate with computers on other networks. It may sometimes be necessary to allow NetBIOS packets to pass through the ZyXEL Device in order to allow computers on the LAN to find computers on the WAN and vice versa. This is the same setting you can set in **Network > WAN > Advanced**.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its default value.

CHAPTER 9
NAT

Use these screens to configure port forwarding and trigger ports for the ZyXEL Device. You can also enable and disable SIP, FTP, and H.323 ALG.

9.1 NAT Overview

9.1.1 Port Forwarding: Services and Port Numbers

A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

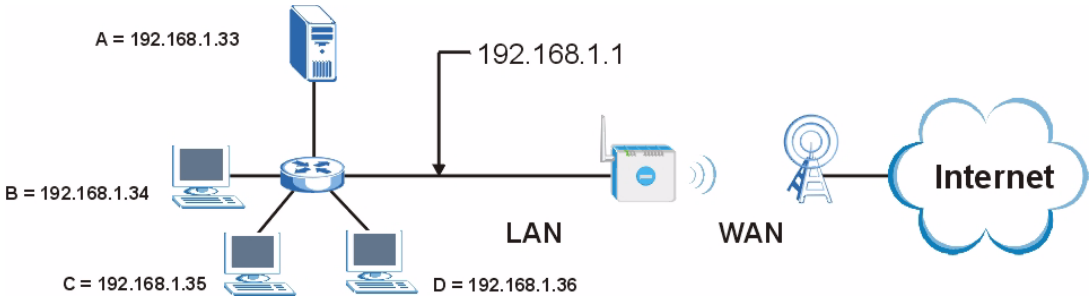
Use the NAT Port Forwarding Screen to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

See Appendix F on page 249 for some examples of services.

For example, let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), port 80 to another (B in the example) and assign a default server IP address of 192.168.1.35 to a third (C in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 53 Multiple Servers Behind NAT Example



9.1.2 Trigger Port Forwarding

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address,

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyXEL Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyXEL Device's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyXEL Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

9.1.2.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding. In this example, **J** is Jane's computer and **S** is the Real Audio server.

Figure 54 Trigger Port Forwarding Process: Example

1. Jane requests a file from the Real Audio server (port 7070).
2. Port 7070 is a "trigger" port and causes the ZyXEL Device to record Jane's computer IP address. The ZyXEL Device associates Jane's computer IP address with the "incoming" port range of 6970-7170.
3. The Real Audio server responds using a port number ranging between 6970-7170.
4. The ZyXEL Device forwards the traffic to Jane's computer IP address.
5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The ZyXEL Device times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

9.1.2.2 Two Points To Remember About Trigger Ports

1. Trigger events only happen on data that is coming from inside the ZyXEL Device and going to the outside.
2. If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

9.1.3 SIP ALG

Some applications, such as SIP, cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload.

Some NAT routers may include a SIP Application Layer Gateway (ALG). An Application Layer Gateway (ALG) manages a specific protocol (such as SIP, H.323 or FTP) at the application layer.

A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream.

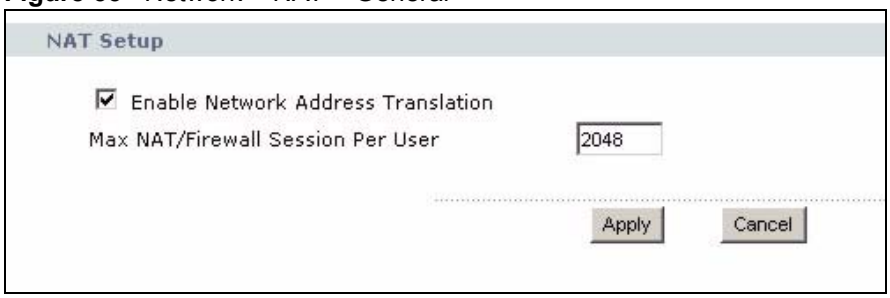
When the ZyXEL Device registers with the SIP register server, the SIP ALG translates the ZyXEL Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy (see Chapter 10 on page 105) if your ZyXEL Device is behind a SIP ALG.

9.2 NAT Screens

9.2.1 NAT General Screen

Use this screen to enable and disable NAT and to allocate memory for NAT and firewall rules. To access this screen, click **Network > NAT > General**.

Figure 55 Network > NAT > General



Each field is described in the following table.

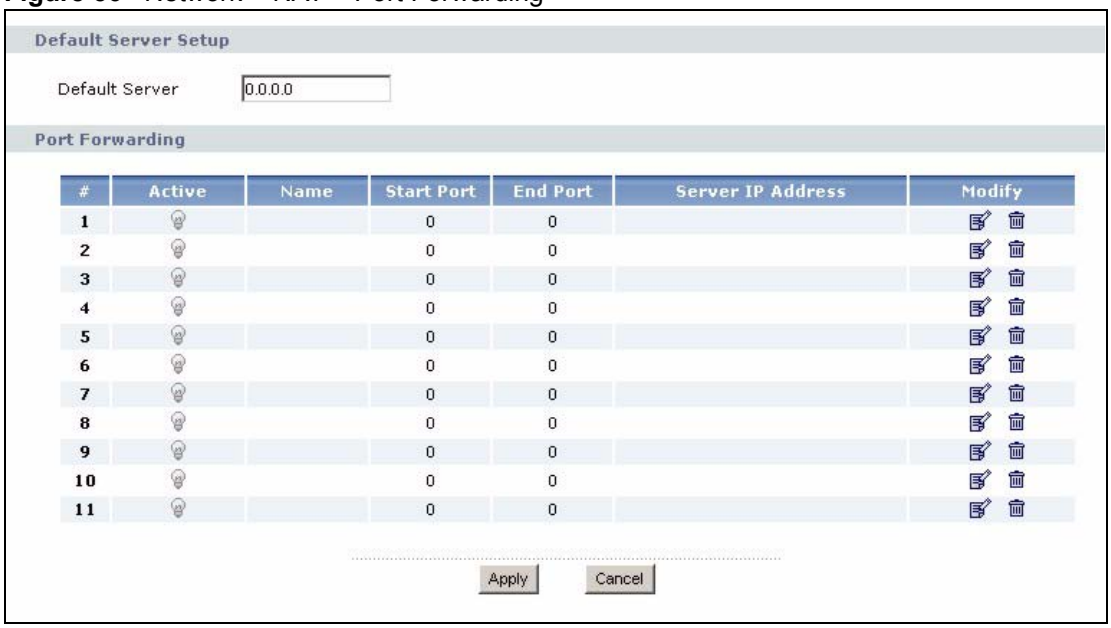
Table 26 Network > NAT > General

LABEL	DESCRIPTION
NAT Setup	
Enable Network Address Translation	Select this if you want to use port forwarding, trigger ports, or any of the ALG.
Max NAT/Firewall Session Per User	When computers use peer to peer applications, such as file sharing applications, they may use a large number of NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet. Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/firewall sessions each client computer can establish through the ZyXEL Device. If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is using all of the available NAT sessions.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

9.2.2 NAT Port Forwarding Screen

Use this screen to look at the current port-forwarding rules in the ZyXEL Device, and to enable, disable, activate, and deactivate each one. You can also set up a default server to handle ports not covered by rules. To access this screen, click **Network > NAT > Port Forwarding**.

Figure 56 Network > NAT > Port Forwarding



Each field is described in the following table.

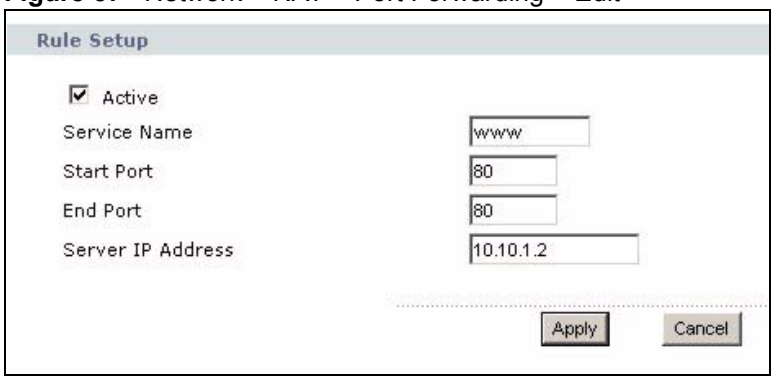
Table 27 Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	Enter the IP address of the server to which the ZyXEL Device should forward packets for ports that are not specified in the **Port Forwarding** section below or in the **Management > Remote MGMT** screens. Enter 0.0.0.0 if you want the ZyXEL Device to discard these packets instead.
Port Forwarding	
#	This field is a sequential value, and it is not associated with a specific rule. The sequence is important, however. The ZyXEL Device checks each rule in order, and it only follows the first one that applies.
Active	Select this to enable this rule. Clear this to disable this rule.
Name	This field displays the name of the rule. It does not have to be unique.
Start Port	This field displays the beginning of the range of port numbers forwarded by this rule.
End Port	This field displays the end of the range of port numbers forwarded by this rule. If it is the same as the **Start Port**, only one port number is forwarded.
Server IP Address	This field displays the IP address of the server to which packet for the selected port(s) are forwarded.
Modify	This column provides icons to edit and delete rules. To edit a rule, click the **Edit** icon next to the rule. The **NAT Port Forwarding Edit** screen appears. To delete a rule, click the **Remove** icon next to the rule. All the information in the rule returns to the default settings.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its last-saved value.

9.2.3 NAT Port Forwarding Edit Screen

Use this screen to activate, deactivate, and edit each port-forwarding rule in the ZyXEL Device. To access this screen, click an **Edit** icon in **Network > NAT > Port Forwarding**.

Figure 57 Network > NAT > Port Forwarding > Edit



Each field is described in the following table.

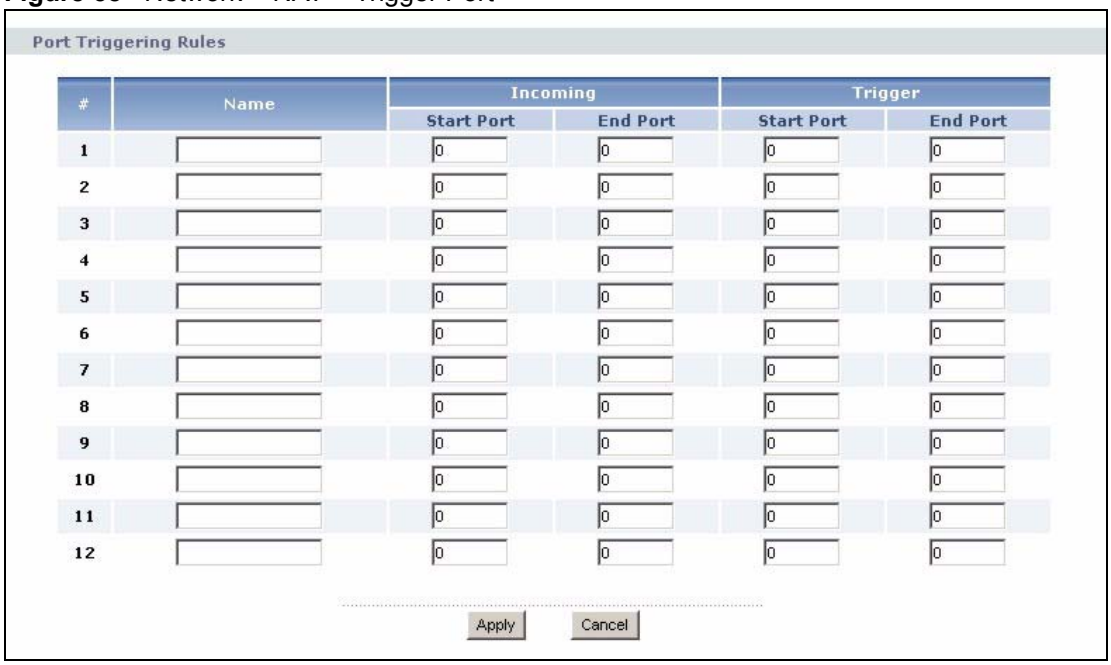
Table 28 Network > NAT > Port Forwarding > Edit

LABEL	DESCRIPTION
Active	Select this to enable this rule. Clear this to disable this rule.
Service Name	Enter a name to identify this rule. You can use 1 - 31 printable ASCII characters, or you can leave this field blank. It does not have to be a unique name.
Start Port End Port	Enter the port number or range of port numbers you want to forward to the specified server. To forward one port number, enter the port number in the **Start Port** and **End Port** fields. To forward a range of ports, • enter the port number at the beginning of the range in the **Start Port** field • enter the port number at the end of the range in the **End Port** field.
Server IP Address	Enter the IP address of the server to which to forward packets for the selected port number(s). This server is usually on the LAN.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

9.2.4 NAT Trigger Port Screen

Use this screen to maintain port-triggering rules in the ZyXEL Device. To access this screen, click **Network > NAT > Trigger Port**.

Figure 58 Network > NAT > Trigger Port



Each field is described in the following table.

Table 29 Network > NAT > Trigger Port

LABEL	DESCRIPTION
Name	Enter a name to identify this rule. You can use 1 - 15 printable ASCII characters, or you can leave this field blank. It does not have to be a unique name.
Incoming	
Start Port End Port	Enter the incoming port number or range of port numbers you want to forward to the IP address the ZyXEL Device records. To forward one port number, enter the port number in the **Start Port** and **End Port** fields. To forward a range of ports, • enter the port number at the beginning of the range in the **Start Port** field • enter the port number at the end of the range in the **End Port** field. If you want to delete this rule, enter zero in the **Start Port** and **End Port** fields.
Trigger	
Start Port End Port	Enter the outgoing port number or range of port numbers that makes the ZyXEL Device record the source IP address and assign it to the selected incoming port number(s). To select one port number, enter the port number in the **Start Port** and **End Port** fields. To select a range of ports, • enter the port number at the beginning of the range in the **Start Port** field • enter the port number at the end of the range in the **End Port** field. If you want to delete this rule, enter zero in the **Start Port** and **End Port** fields.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to discard your changes.

9.2.5 NAT ALG Screen

Use this screen to enable and disable SIP (VoIP), FTP (file transfer), and H.323 (audio-visual) ALG in the ZyXEL Device. To access this screen, click **Network > NAT > ALG**.

Figure 59 Network > NAT > ALG

Each field is described in the following table.

Table 30 Network > NAT > ALG

LABEL	DESCRIPTION
Enable SIP ALG	Select this to make sure SIP (VoIP) works correctly with port-forwarding and port-triggering rules.
Enable FTP ALG	Select this to make sure FTP (file transfer) works correctly with port-forwarding and port-triggering rules.
Enable H.323 ALG	Select this to make sure H.323 (audio-visual programs, such as NetMeeting) works correctly with port-forwarding and port-triggering rules.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to discard your most recent changes.

CHAPTER 10
SIP

Use these screens to set up your SIP accounts and to configure QoS settings.

10.1 SIP Overview

10.1.1 Introduction to VoIP

VoIP (Voice over IP) is the sending of voice signals over the Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service. A company could alternatively set up an IP-PBX and provide it's own VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

10.1.2 Introduction to SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

10.1.3 SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

10.1.3.1 SIP Number

The SIP number is the part of the SIP URI that comes before the "@" symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

10.1.3.2 SIP Service Domain

The SIP service domain of the VoIP service provider (the company that lets you make phone calls over the Internet) is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then "VoIP-provider.com" is the SIP service domain.

10.1.4 SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 31 SIP Call Progression

A		B
1. INVITE		
		2. Ringing
		3. OK
4. ACK		
	5.Dialogue (voice traffic)	
6. BYE		
		7. OK

1. A sends a SIP INVITE request to B. This message is an invitation for B to participate in a SIP telephone call.
2. B sends a response indicating that the telephone is ringing.
3. B sends an OK response after the call is answered.
4. A then sends an ACK message to acknowledge that B has answered the call.
5. Now A and B exchange voice media (talk).
6. After talking, A hangs up and sends a BYE request.
7. B replies with an OK response confirming receipt of the BYE request and the call is terminated.

10.1.5 SIP Client Server

SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

10.1.5.1 SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either A or B can act as a SIP user agent client to initiate a call. A and B can also both act as a SIP user agent to receive the call.

Figure 60 SIP User Agent

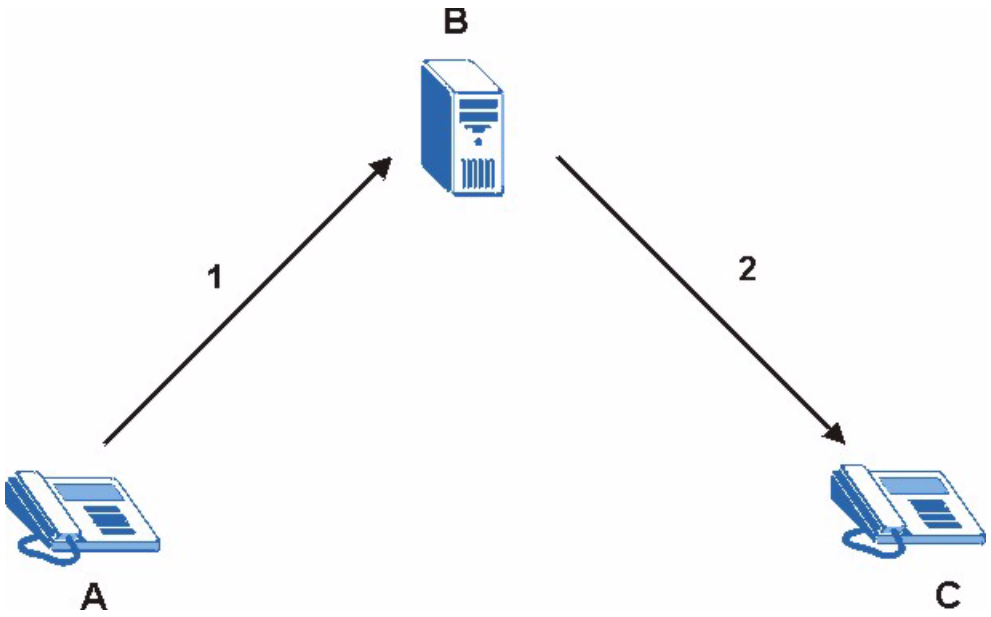
10.1.5.2 SIP Proxy Server

A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device A to call someone who is using client device C.

1. The client device (A in the figure) sends a call invitation to the SIP proxy server (B).
2. The SIP proxy server forwards the call invitation to C.

Figure 61 SIP Proxy Server



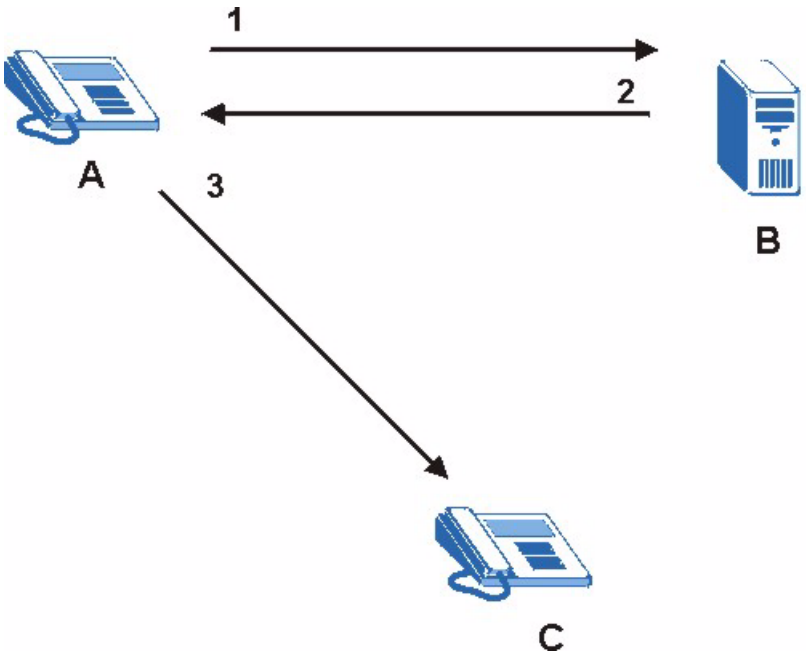
10.1.5.3 SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

In the following example, you want to use client device A to call someone who is using client device C.

1. Client device A sends a call invitation for C to the SIP redirect server (B).
2. The SIP redirect server sends the invitation back to A with C's IP address (or domain name).
3. Client device A then sends the call invitation to client device C.

Figure 62 SIP Redirect Server



10.1.5.4 SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

10.1.6 RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

10.1.7 NAT and SIP

The ZyXEL Device must register its public IP address with a SIP register server. If there is a NAT router between the ZyXEL Device and the SIP register server, the ZyXEL Device probably has a private IP address. The ZyXEL Device lists its IP address in the SIP message that it sends to the SIP register server. NAT does not translate this IP address in the SIP message. The SIP register server gets the ZyXEL Device's IP address from inside the SIP message and maps it to your SIP identity. If the ZyXEL Device has a private IP address listed in the SIP message, the SIP server cannot map it to your SIP identity. See Chapter 9 on page 97 for more information about NAT.

Use a SIP ALG (Application Layer Gateway), Use NAT, STUN, or outbound proxy to allow the ZyXEL Device to list its public IP address in the SIP messages.

10.1.7.1 SIP ALG

See Section 9.1.3 on page 99.

10.1.7.2 Use NAT

If you know the NAT router's public IP address and SIP port number, you can use the Use NAT feature to manually configure the ZyXEL Device to use a them in the SIP messages. This eliminates the need for STUN or a SIP ALG.

You must also configure the NAT router to forward traffic with this port number to the ZyXEL Device.

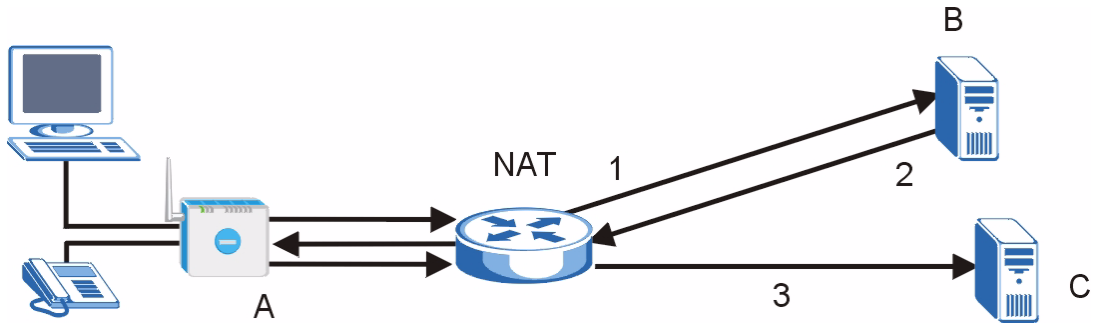
10.1.7.3 STUN

STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the ZyXEL Device to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the ZyXEL Device to find the public IP address that NAT assigned, so the ZyXEL Device can embed it in the SIP data stream. STUN does not work with symmetric NAT routers or firewalls. See RFC 3489 for details on STUN.

The following figure shows how STUN works.

1. The ZyXEL Device (A) sends SIP packets to the STUN server (B).
2. The STUN server (B) finds the public IP address and port number that the NAT router used on the ZyXEL Device's SIP packets and sends them to the ZyXEL Device.
3. The ZyXEL Device uses the public IP address and port number in the SIP packets that it sends to the SIP server (C).

Figure 63 STUN



10.1.7.4 Outbound Proxy

Your VoIP service provider may host a SIP outbound proxy server to handle all of the ZyXEL Device's VoIP traffic. This allows the ZyXEL Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off a SIP ALG on a NAT router in front of the ZyXEL Device to keep it from retranslating the IP address (since this is already handled by the outbound proxy server).

10.1.8 Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into voice signals. The ZyXEL Device supports the following codecs.

- **G.711** is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals (sampling) and converts them into digital bits (quantization). Quantization "reads" the analog signal and then "writes" it to the nearest digital value. For this reason, a digital sample is usually slightly different from its analog original (this difference is known as "quantization noise").

  G.711 provides excellent sound quality but requires 64kbps of bandwidth.

- **G.723** is an Adaptive Differential Pulse Code Modulation (ADPCM) waveform codec. Differential (or Delta) PCM is similar to PCM, but encodes the audio signal based on the difference between one sample and a prediction based on previous samples, rather than encoding the sample's actual quantized value. Many thousands of samples are taken each second, and the differences between consecutive samples are usually quite small, so this saves space and reduces the bandwidth necessary.

  However, DPCM produces a high quality signal (high signal-to-noise ratio or SNR) for high difference signals (where the actual signal is very different from what was predicted) but a poor quality signal (low SNR) for low difference signals (where the actual signal is very similar to what was predicted). This is because the level of quantization noise is the same at all signal levels. Adaptive DPCM solves this problem by adapting the difference signal's level of quantization according to the audio signal's strength. A low difference signal is given a higher quantization level, increasing its signal-to-noise ratio. This provides a similar sound quality at all signal levels.

  G.723 provides high quality sound and requires 20 or 40 kbps.

- **G.729** is an Analysis-by-Synthesis (AbS) hybrid waveform codec. It uses a filter based on information about how the human vocal tract produces sounds. The codec analyzes the incoming voice signal and attempts to synthesize it using its list of voice elements. It tests the synthesized signal against the original and, if it is acceptable, transmits details of the voice elements it used to make the synthesis. Because the codec at the receiving end has the same list, it can exactly recreate the synthesized audio signal.

  G.729 provides good sound quality and reduces the required bandwidth to 8kbps.

10.1.9 PSTN Call Setup Signaling

PSTNs (Public Switched Telephone Networks) use DTMF or pulse dialing to set up telephone calls.

Dual-Tone Multi-Frequency (DTMF) signaling uses pairs of frequencies (one lower frequency and one higher frequency) to set up calls. It is also known as Touch Tone®. Each of the keys on a DTMF telephone corresponds to a different pair of frequencies.

Pulse dialing sends a series of clicks to the local phone office in order to dial numbers.[1]

10.1.10 MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message–waiting (beeping) dial tone when you have one or more voice messages. Your VoIP service provider must have a messaging system that sends message-waiting-status SIP packets as defined in RFC 3842.

10.1.11 Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the ZyXEL Device. The ZyXEL Device allows you to record custom tones for the **Caller Ringing Tone** and **On Hold Tone** functions. The same recordings apply to both the caller ringing and on hold tones.

Table 32 Custom Tones Details

LABEL	DESCRIPTION
Total Time for All Tones	128 seconds for all custom tones combined
Maximum Time per Individual Tone	20 seconds
Total Number of Tones Recordable	8 You can record up to eight different custom tones but the total time must be 128 seconds or less.

1. The ZyXEL Device supports DTMF at the time of writing.

10.1.11.1 Recording Custom Tones

Use the following steps if you would like to create new tones or change your tones:

1. Pick up the phone and press ******** on your phone's keypad and wait for the message that says you are in the configuration menu.
2. Press a number from 1101~1108 on your phone followed by the # key.
3. Play your desired music or voice recording into the receiver's mouthpiece. Press the # key.
4. You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

10.1.11.2 Listening to Custom Tones

Do the following to listen to a custom tone:

1. Pick up the phone and press ******** on your phone's keypad and wait for the message that says you are in the configuration menu.
2. Press a number from 1201~1208 followed by the # key to listen to the tone.
3. You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

10.1.11.3 Deleting Custom Tones

Do the following to delete a custom tone:

1. Pick up the phone and press ******** on your phone's keypad and wait for the message that says you are in the configuration menu.
2. Press a number from 1301~1308 followed by the # key to delete the tone of your choice. Press 14 followed by the # key if you wish to clear all your custom tones.
3. You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

10.1.12 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay and the networking methods used to provide bandwidth for real-time multimedia applications.

10.1.12.1 Type Of Service (ToS)

Network traffic can be classified by setting the ToS (Type Of Service) values at the data source (for example, at the ZyXEL Device) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

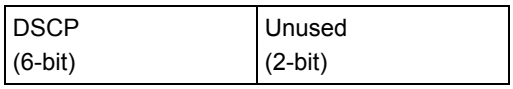
10.1.12.2 DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.[1]

10.1.12.3 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

Figure 64 DiffServ: Differentiated Service Field



DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

10.1.12.4 VLAN

Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Only stations within the same group can communicate with each other.

Your ZyXEL Device can add IEEE 802.1Q VLAN ID tags to voice frames that it sends to the network. This allows the ZyXEL Device to communicate with a SIP server that is a member of the same VLAN group. Some ISPs use the VLAN tag to identify voice traffic and give it priority over other traffic.

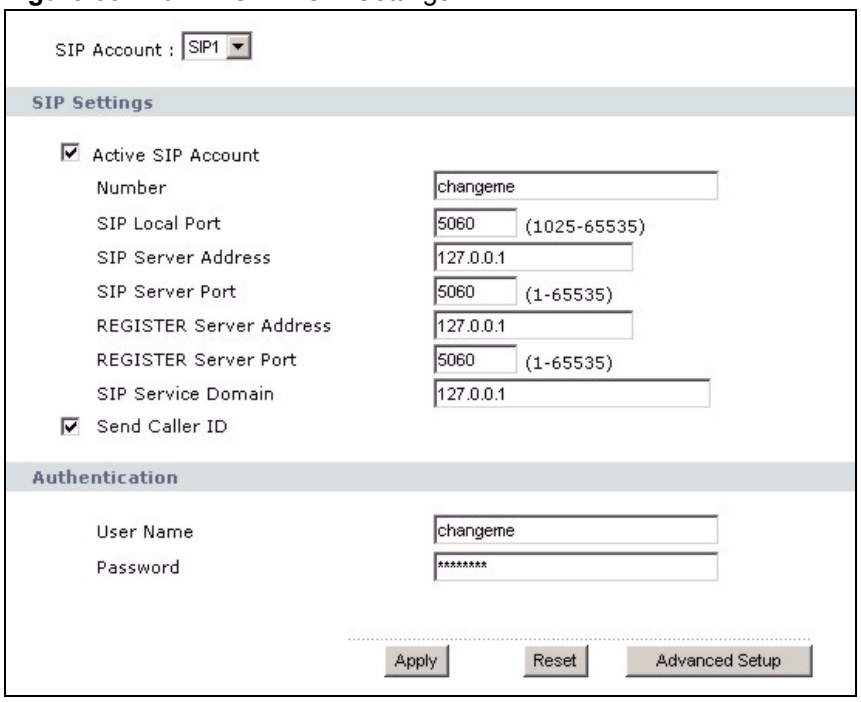
1. The ZyXEL Device does not support DiffServ at the time of writing.

10.2 SIP Screens

10.2.1 SIP Settings Screen

Use this screen to maintain basic information about each SIP account. Your VoIP service provider (the company that lets you make phone calls over the Internet) should provide this. You can also enable and disable each SIP account. To access this screen, click **VoIP > SIP > SIP Settings**.

Figure 65 VoIP > SIP > SIP Settings



Each field is described in the following table.

Table 33 VoIP > SIP > SIP Settings

LABEL	DESCRIPTION
SIP Account	Select the SIP account you want to see in this screen. If you change this field, the screen automatically refreshes.
SIP Settings	
Active SIP Account	Select this if you want the ZyXEL Device to use this account. Clear it if you do not want the ZyXEL Device to use this account.
Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters.
SIP Local Port	Enter the ZyXEL Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.

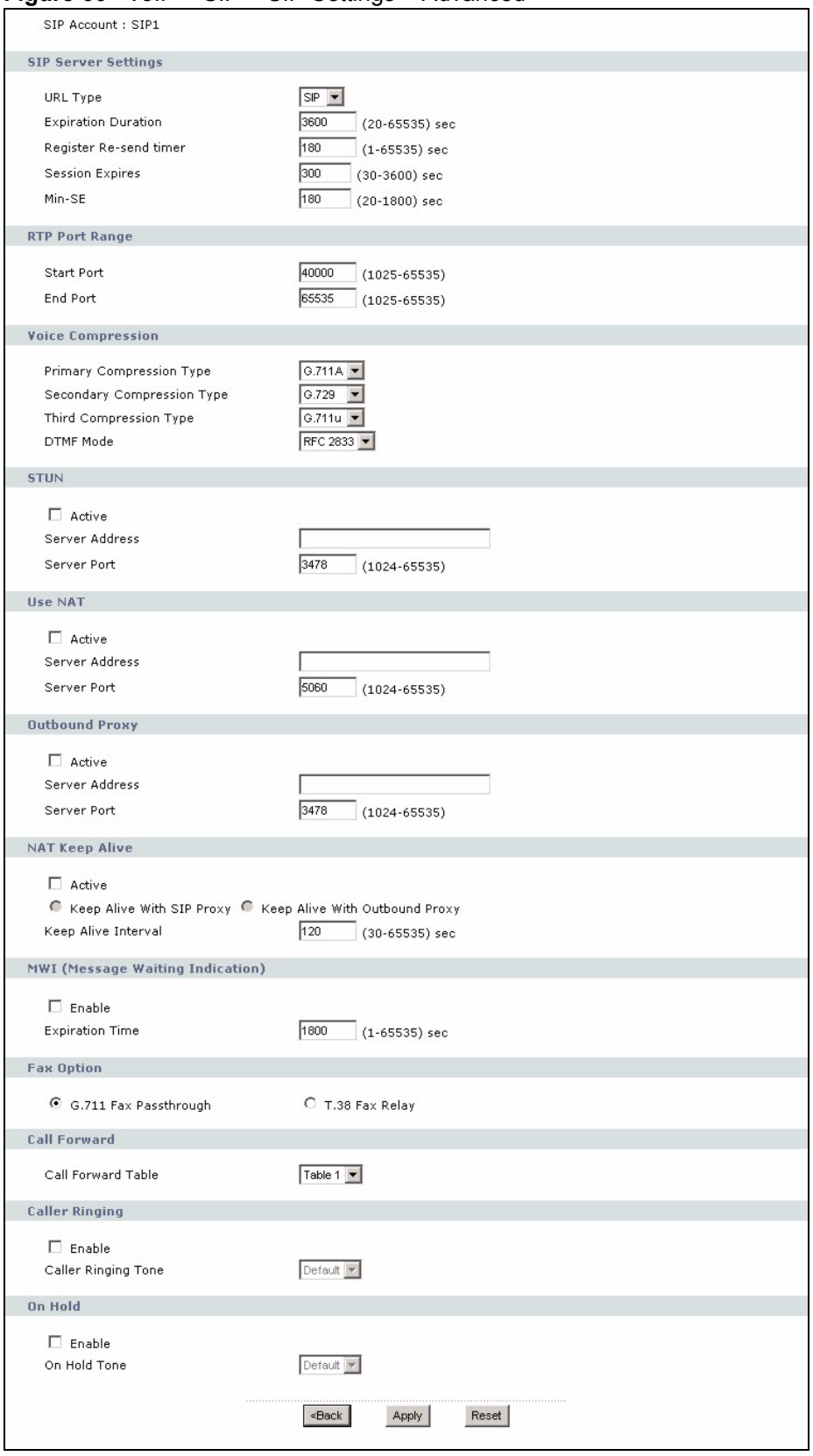
Table 33 VoIP > SIP > SIP Settings

LABEL	DESCRIPTION
SIP Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the **SIP Server Address** field. You can use up to 95 printable ASCII characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the **SIP Server Port** field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Authentication	
User Name	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
Password	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII Extended set characters.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.
Advanced Setup	Click this to edit the advanced settings for this SIP account. The **Advanced SIP Setup** screen appears.

10.2.2 Advanced SIP Setup Screen

Use this screen to maintain advanced settings for each SIP account. To access this screen, click **Advanced Setup** in **VoIP > SIP > SIP Settings**.

Figure 66 VoIP > SIP > SIP Settings > Advanced



Each field is described in the following table.

Table 34 VoIP > SIP > SIP Settings > Advanced

LABEL	DESCRIPTION
SIP Account	This field displays the SIP account you see in this screen.
SIP Server Settings	
URL Type	Select whether or not to include the SIP service domain name when the ZyXEL Device sends the SIP number. **SIP** - include the SIP service domain name **TEL** - do not include the SIP service domain name
Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The ZyXEL Device automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.)
Register Re-send timer	Enter the number of seconds the ZyXEL Device waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires	Enter the number of seconds the conversation can last before the call is automatically disconnected. Usually, when one-half of this time has passed, the ZyXEL Device or the other party updates this timer to prevent this from happening.
Min-SE	Enter the minimum number of seconds the ZyXEL Device accepts for a session expiration time when it receives a request to start a SIP session. If the request has a shorter time, the ZyXEL Device rejects it.
RTP Port Range	
Start Port End Port	Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the **Start Port** and **End Port** fields. To enter a range of ports, • enter the port number at the beginning of the range in the **Start Port** field • enter the port number at the end of the range in the **End Port** field.
Voice Compression	Select the type of voice coder/decoder (codec) that you want the ZyXEL Device to use. G.711 provides high voice quality but requires more bandwidth (64 kbps). • **G.711A** is typically used in Europe. • **G.711u** is typically used in North America and Japan. **G.723** provides good voice quality, and requires 20 or 40 kbps. In contrast, **G.729** requires only 8 kbps. The ZyXEL Device must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec.
Primary Compression Type	Select the ZyXEL Device's first choice for voice coder/decoder.
Secondary Compression Type	Select the ZyXEL Device's second choice for voice coder/decoder. Select **None** if you only want the ZyXEL Device to accept the first choice.
Third Compression Type	This field is disabled if **Secondary Compression Type** is **None**. Select the ZyXEL Device's third choice for voice coder/decoder. Select **None** if you only want the ZyXEL Device to accept the first or second choice.

Table 34 VoIP > SIP > SIP Settings > Advanced

LABEL	DESCRIPTION
DTMF Mode	Control how the ZyXEL Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses. **RFC 2833** - send the DTMF tones in RTP packets **PCM** - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) can distort the tones. **SIP INFO** - send the DTMF tones in SIP messages
STUN	
Active	Select this if all of the following conditions are satisfied. • There is a NAT router between the ZyXEL Device and the SIP server. • The NAT router is not a SIP ALG. • Your VoIP service provider gave you an IP address or domain name for a STUN server. Otherwise, clear this field.
Server Address	Enter the IP address or domain name of the STUN server provided by your VoIP service provider.
Server Port	Enter the STUN server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
Use NAT	
Active	Select this if you want the ZyXEL Device to send SIP traffic to a specific NAT router. You must also configure the NAT router to forward traffic with the specified port to the ZyXEL Device. This eliminates the need for STUN or a SIP ALG.
Server Address	Enter the public IP address or domain name of the NAT router.
Server Port	Enter the port number that your SIP sessions use with the public IP address of the NAT router.
Outbound Proxy	
Active	Select this if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the ZyXEL Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the ZyXEL Device to keep it from retranslating the IP address (since this is already handled by the outbound proxy server).
Server Address	Enter the IP address or domain name of the SIP outbound proxy server.
Server Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
NAT Keep Alive	
Active	Select this to stop NAT routers between the ZyXEL Device and SIP server (a SIP proxy server or outbound proxy server) from dropping the SIP session. The ZyXEL Device does this by sending SIP notify messages to the SIP server based on the specified interval.
Keep Alive with SIP Proxy	Select this if the SIP server is a SIP proxy server.
Keep Alive with Outbound Proxy	Select this if the SIP server is an outbound proxy server. You must enable **Outbound Proxy** to use this.
Keep Alive Interval	Enter how often (in seconds) the ZyXEL Device should send SIP notify messages to the SIP server.

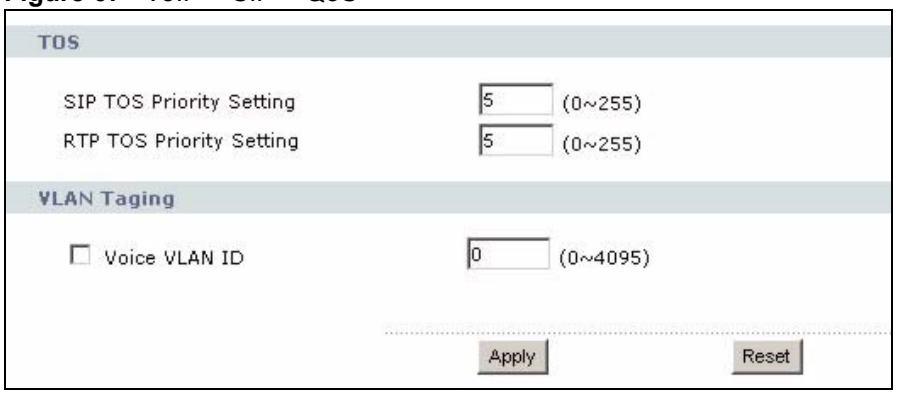
Table 34 VoIP > SIP > SIP Settings > Advanced

LABEL	DESCRIPTION
MWI (Message Waiting Indication)	
Enable	Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your VoIP service provider must support this feature.
Expiration Time	Keep the default value, unless your VoIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the ZyXEL Device subscribes to the service. Before this time passes, the ZyXEL Device automatically subscribes again.
Fax Option	This field controls how the ZyXEL Device handles fax messages.
G.711 Fax Passthrough	Select this if the ZyXEL Device should use G.711 to send fax messages. The peer devices must also use G.711.
T.38 Fax Relay	Select this if the ZyXEL Device should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38.
Call Forward	
Call Forward Table	Select which call forwarding table you want the ZyXEL Device to use for incoming calls. You set up these tables in **VoIP > Phone Book > Incoming Call Policy**.
Caller Ringing	
Enable	Check this box if you want people to hear a customized recording when they call you.
Caller Ringing Tone	Select the tone you want people to hear when they call you. See Section 10.1.11 on page 111 for information on how to record these tones.
On Hold	
Enable	Check this box if you want people to hear a customized recording when you put them on hold.
On Hold Tone	Select the tone you want people to hear when you put them on hold. See Section 10.1.11 on page 111 for information on how to record these tones.
<Back	Click this to return to the **SIP Settings** screen without saving your changes.
Apply	Click this to save your changes.
Cancel	Click this to set every field in this screen to its last-saved value.

10.2.3 SIP QoS Screen

Use this screen to maintain ToS and VLAN settings for the ZyXEL Device. To access this screen, click **VoIP > SIP > QoS**.

Figure 67 VoIP > SIP > QoS



Each field is described in the following table.

Table 35 VoIP > SIP > QoS

LABEL	DESCRIPTION
SIP TOS Priority Setting	Enter the priority for SIP voice transmissions. The ZyXEL Device creates Type of Service priority tags with this priority to voice traffic that it transmits.
RTP TOS Priority Setting	Enter the priority for RTP voice transmissions. The ZyXEL Device creates Type of Service priority tags with this priority to RTP traffic that it transmits.
Voice VLAN ID	Select this if the ZyXEL Device has to be a member of a VLAN to communicate with the SIP server. Ask your network administrator, if you are not sure. Enter the VLAN ID provided by your network administrator in the field on the right. Your LAN and gateway must be configured to use VLAN tags. Otherwise, clear this field.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

CHAPTER 11
Phone

Use these screens to configure the phone you use to make phone calls with the ZyXEL Device.

11.1 Phone Overview

You can configure the volume, echo cancellation, VAD settings and custom tones for the phone port on the ZyXEL Device. You can also select which SIP account to use for making outgoing calls.

11.1.1 Voice Activity Detection/Silence Suppression/Comfort Noise

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the ZyXEL Device reduce the bandwidth that a call uses by not transmitting "silent packets" when you are not speaking.

When using VAD, the ZyXEL Device generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

11.1.2 Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

11.1.3 Supplementary Phone Services Overview

Supplementary services such as call hold, call waiting, call transfer, etc. are generally available from your VoIP service provider. The ZyXEL Device supports the following services:

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding
- Three-Way Conference
- Internal Calls
- Caller ID

- CLIP (Calling Line Identification Presentation)
- CLIR (Calling Line Identification Restriction)

Note: To take full advantage of the supplementary phone services available though the ZyXEL Device's phone port, you may need to subscribe to the services from your VoIP service provider.

11.1.3.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. The ZyXEL Device may interpret manual tapping as hanging up if the duration is too long

You can invoke all the supplementary services by using the flash key.

11.1.3.2 Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 36 European Type Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

11.1.3.2.1 European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then "2" to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then "0" to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then "1" to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

11.1.3.2.2 European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.

  Press the flash key and then press "0".
- Disconnect the first call and answer the second call.

  Either press the flash key and press "1", or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.

  Press the flash key and then "2".

11.1.3.2.3 European Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1. Press the flash key to put the caller on hold.
2. When you hear the dial tone, dial "*98#" followed by the number to which you want to transfer the call. to operate the Intercom.
3. After you hear the ring signal or the second party answers it, hang up the phone.

11.1.3.2.4 European Three-Way Conference

Use the following steps to make three-way conference calls.

1. When you are on the phone talking to someone, place the flash key to put the caller on hold and get a dial tone.
2. Dial a phone number directly to make another call.
3. When the second call is answered, press the flash key and press "3" to create a three-way conversation.
4. Hang up the phone to drop the connection.

5 If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press "2".

11.1.3.3 USA Type Supplementary Services

This section describes how to use supplementary phone services with the **USA Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 37 USA Type Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. After the second call is successful, press the flash key again to have a three-way conference call. Put a current call on hold to answer an incoming call.
Flash	*98#	Transfer the call to another phone.

11.1.3.3.1 USA Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key to switch back and forth between caller **A** and **B** by putting either one on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

11.1.3.3.2 USA Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to your telephone number, you will hear a call waiting tone.

Press the flash key to put the first call on hold and answer the second call.

11.1.3.3.3 USA Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1 Press the flash key to put the caller on hold.

2 When you hear the dial tone, dial "*98#" followed by the number to which you want to transfer the call. to operate the Intercom.

3 After you hear the ring signal or the second party answers it, hang up the phone.

11.1.3.3.4 USA Three-Way Conference

Use the following steps to make three-way conference calls.

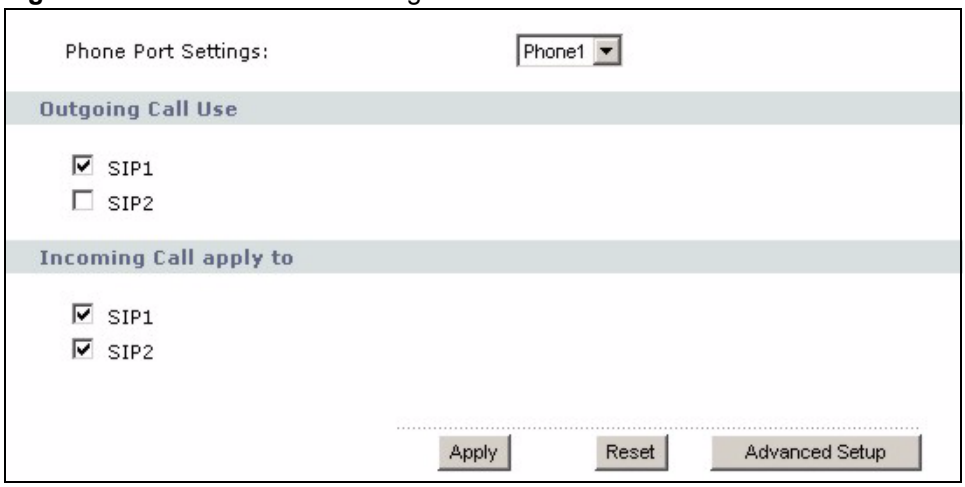
1. When you are on the phone talking to someone, place the flash key to put the caller on hold and get a dial tone.
2. Dial a phone number directly to make another call.
3. When the second call is answered, press the flash key, wait for the sub-command tone and press "3" to create a three-way conversation.
4. Hang up the phone to drop the connection.
5. If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key, wait for the sub-command tone and press "2".

11.2 Phone Screens

11.2.1 Analog Phone Screen

Use this screen to control which SIP accounts and PSTN line each phone uses. To access this screen, click **VoIP > Phone > Analog Phone**.

Figure 68 VoIP > Phone > Analog Phone



Each field is described in the following table.

Table 38 VoIP > Phone > Analog Phone

LABEL	DESCRIPTION
Phone Port Settings	Select the phone port you want to see in this screen. If you change this field, the screen automatically refreshes.
Outgoing Call Use	

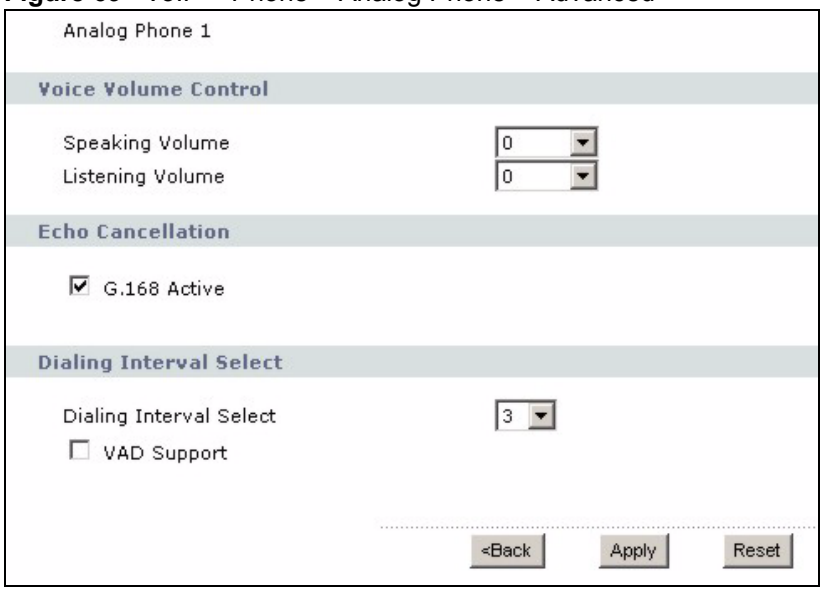
Table 38 VoIP > Phone > Analog Phone

LABEL	DESCRIPTION
SIP1	Select this if you want this phone port to use the SIP1 account when it makes calls. If you select both SIP accounts, the ZyXEL Device tries to use SIP2 first.
SIP2	Select this if you want this phone port to use the SIP2 account when it makes calls. If you select both SIP accounts, the ZyXEL Device tries to use SIP2 first.
Incoming Call apply to	
SIP1	Select this if you want to receive phone calls for the SIP1 account on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls.
SIP2	Select this if you want to receive phone calls for the SIP2 account on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.
Advanced Setup	Click this to edit the advanced settings for this phone port. The **Advanced Analog Phone Setup** screen appears.

11.2.2 Advanced Analog Phone Setup Screen

Use this screen to edit advanced settings for each phone port. To access this screen, click **Advanced Setup** in **VoIP > Phone > Analog Phone**.

Figure 69 VoIP > Phone > Analog Phone > Advanced



Each field is described in the following table.

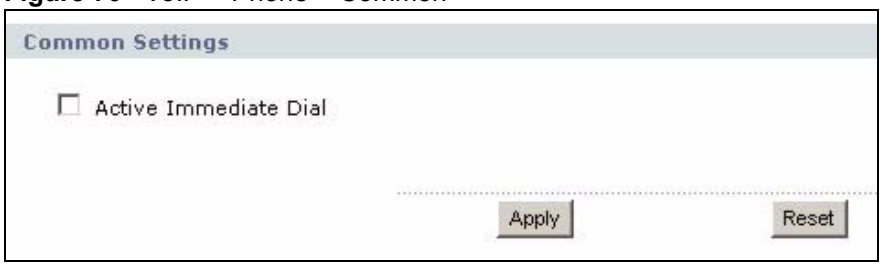
Table 39 VoIP > Phone > Analog Phone > Advanced

LABEL	DESCRIPTION
Analog Phone	This field displays the phone port you see in this screen.
Voice Volume Control	
Speaking Volume	Enter the loudness that the ZyXEL Device uses for speech that it sends to the peer device. -1 is the quietest, and 1 is the loudest.
Listening Volume	Enter the loudness that the ZyXEL Device uses for speech that it receives from the peer device. -1 is the quietest, and 1 is the loudest.
Echo Cancellation	
G.168 Active	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Dialing Interval Select	
Dialing Interval Select	Enter the number of seconds the ZyXEL Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers. If you select **Active Immediate Dial** in **VoIP > Phone > Common**, you can press the pound key (#) to tell the ZyXEL Device to make the phone call immediately, regardless of this setting.
VAD Support	Select this if the ZyXEL Device should stop transmitting when you are not speaking. This reduces the bandwidth the ZyXEL Device uses.
<Back	Click this to return to the **Analog Phone** screen without saving your changes.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its last-saved value.

11.2.3 Common Phone Settings Screen

Use this screen to activate and deactivate immediate dialing. To access this screen, click **VoIP > Phone > Common**.

Figure 70 VoIP > Phone > Common



Each field is described in the following table.

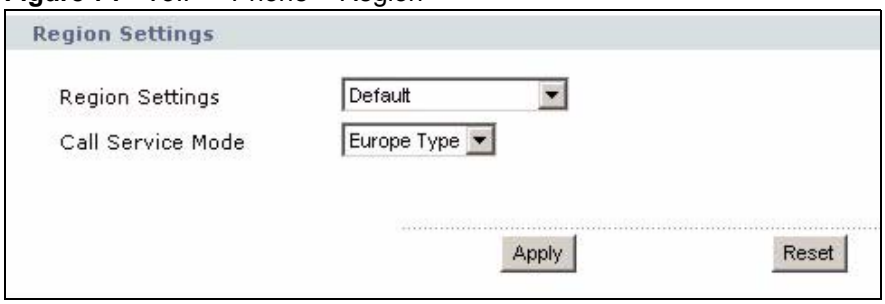
Table 40 VoIP > Phone > Common

LABEL	DESCRIPTION
Active Immediate Dial	Select this if you want to use the pound key (#) to tell the ZyXEL Device to make the phone call immediately, instead of waiting the number of seconds you selected in the **Dialing Interval Select** in **VoIP > Phone > Analog Phone**. If you select this, dial the phone number, and then press the pound key if you do not want to wait. The ZyXEL Device makes the call immediately.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

11.2.4 Phone Region Screen

Use this screen to maintain settings that often depend on which region of the world the ZyXEL Device is in. To access this screen, click **VoIP > Phone > Region**.

Figure 71 VoIP > Phone > Region



Each field is described in the following table.

Table 41 VoIP > Phone > Region

LABEL	DESCRIPTION
Region Settings	Select the place in which the ZyXEL Device is located. Do not select **Default**.
Call Service Mode	Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. **Europe Type** - use supplementary phone services in European mode **USA Type** - use supplementary phone services American mode You might have to subscribe to these services to use them. Contact your VoIP service provider.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its last-saved value.

CHAPTER 12
Firewall

Use these screens to enable, configure and disable the firewall that protects your ZyXEL Device and your LAN from unwanted or malicious traffic.

12.1 Firewall Overview

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

12.1.1 Stateful Inspection Firewall.

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

12.1.2 About the ZyXEL Device Firewall

The ZyXEL Device firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated. The ZyXEL Device's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyXEL Device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The ZyXEL Device is installed between the LAN and a WiMAX base station connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

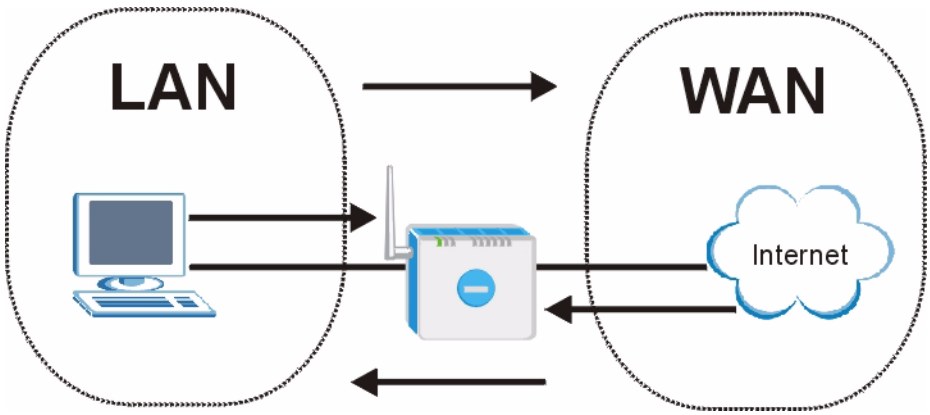
The ZyXEL Device has one Ethernet (LAN) port. The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

12.1.3 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via web configurator.
2. Think about access control before you connect to the network in any way.
3. Limit who can access your router.
4. Don't enable any local service (such as telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

12.1.4 The Firewall, NAT and Remote Management

Figure 72 Firewall Rule Directions



12.1.4.1 LAN-to-WAN rules

LAN-to-WAN rules are local network to Internet firewall rules. The default is to forward all traffic from your local network to the Internet.

You can block certain **LAN-to-WAN** traffic in the **Services** screen (click the **Services** tab). All services displayed in the **Blocked Services** list box are **LAN-to-WAN** firewall rules that block those services originating from the LAN.

Blocked **LAN-to-WAN** packets are considered alerts. Alerts are "higher priority logs" that include system errors, attacks and attempted access to blocked web sites. Alerts appear in red in the **View Log** screen. You may choose to have alerts e-mailed immediately in the **Log Settings** screen.

LAN-to-LAN/ZyXEL Device means the LAN to the ZyXEL Device LAN interface. This is always allowed, as this is how you manage the ZyXEL Device from your local computer.

12.1.4.2 WAN-to-LAN rules

WAN-to-LAN rules are Internet to your local network firewall rules. The default is to block all traffic from the Internet to your local network.

How can you forward certain WAN to LAN traffic? You may allow traffic originating from the WAN to be forwarded to the LAN by:

- Configuring NAT port forwarding rules.
- Configuring **One-to-One** and **Many-One-to-One** NAT mapping rules in the SMT NAT menus.
- Configuring **WAN** or **LAN & WAN** access for services in the **Remote Management** screens or SMT menus. When you allow remote management from the WAN, you are actually configuring WAN-to-WAN/ZyXEL Device firewall rules. WAN-to-WAN/ ZyXEL Device firewall rules are Internet to the ZyXEL Device WAN interface firewall rules. The default is to block all such traffic. When you decide what WAN-to-LAN packets to log, you are in fact deciding what **WAN-to-LAN** and WAN-to-WAN/ZyXEL Device packets to log.

Forwarded **WAN-to-LAN** packets are not considered alerts.

12.2 Triangle Route

When the firewall is on, your ZyXEL Device acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the ZyXEL Device to protect your LAN against attacks.

Figure 73 Ideal Firewall Setup

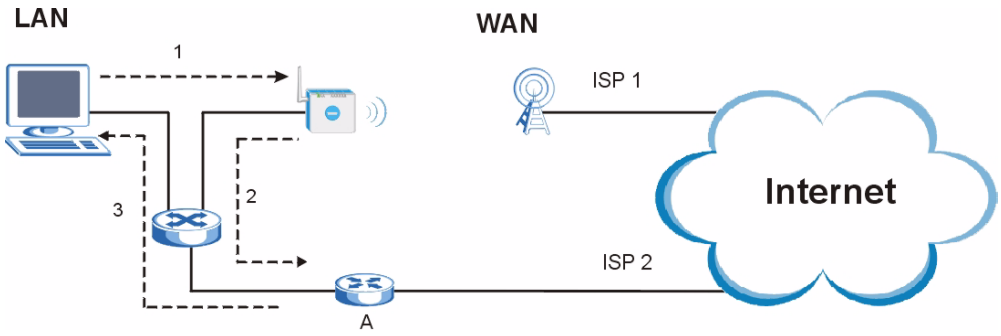
12.2.1 The "Triangle Route" Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. You may have more than one connection to the Internet (through one or more ISPs). If an alternate gateway is on the LAN (and its IP address is in the same subnet as the ZyXEL Device's LAN IP address), the "triangle route" (also called asymmetrical route) problem may occur. The steps below describe the "triangle route" problem.

1. A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.
2. The ZyXEL Device reroutes the SYN packet through Gateway **A** on the LAN to the WAN.
3. The reply from the WAN goes directly to the computer on the LAN without going through the ZyXEL Device.

As a result, the ZyXEL Device resets the connection, as the connection has not been acknowledged.

Figure 74 "Triangle Route" Problem



12.2.2 Solving the "Triangle Route" Problem

If you have the ZyXEL Device allow triangle route sessions, traffic from the WAN can go directly to a LAN computer without passing through the ZyXEL Device and its firewall protection.

Another solution is to use IP alias. IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your ZyXEL Device supports up to three logical LAN interfaces with the ZyXEL Device being the gateway for each logical network.

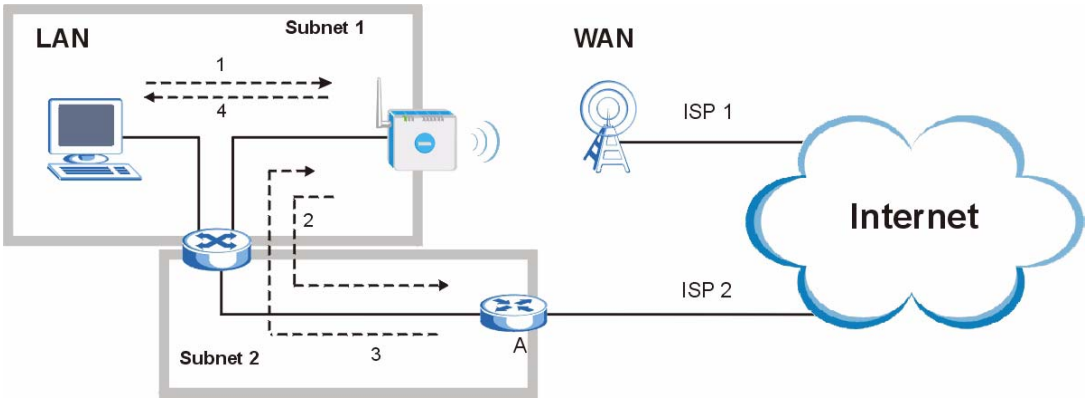
It's like having multiple LAN networks that actually use the same physical cables and ports. By putting your LAN and Gateway **A** in different subnets, all returning network traffic must pass through the ZyXEL Device to your LAN. The following steps describe such a scenario.

1. A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
2. The ZyXEL Device reroutes the packet to Gateway A, which is in Subnet 2.

3 The reply from the WAN goes to the ZyXEL Device.

4 The ZyXEL Device then sends it to the computer on the LAN in Subnet 1.

Figure 75 IP Alias

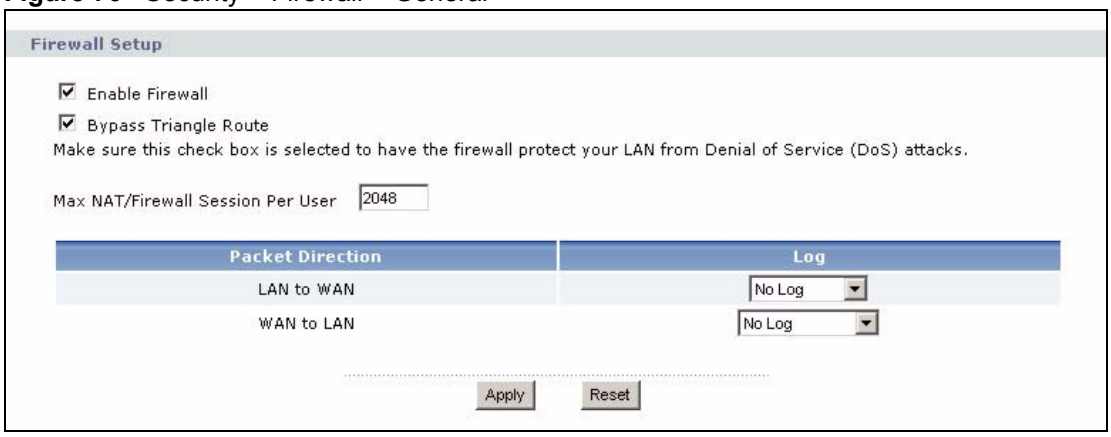


12.3 Firewall Screens

12.3.1 General Firewall Screen

Use this screen to configure the basic settings for your firewall. To access this screen, click **Security > Firewall > General**.

Figure 76 Security > Firewall > General



Each field is described in the following table.

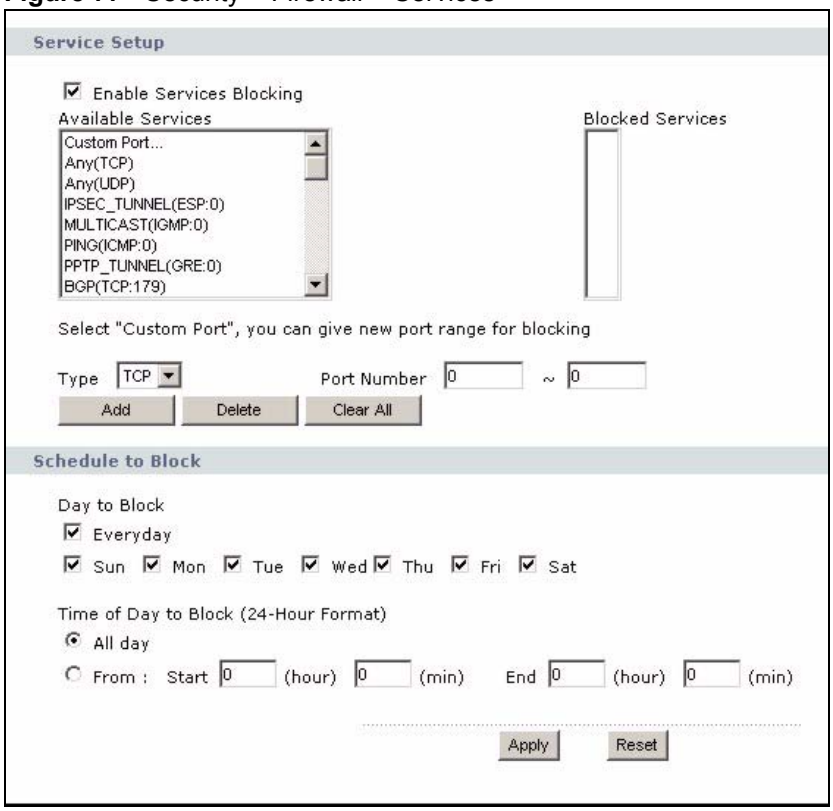
Table 42 Security > Firewall > General

LABEL	DESCRIPTION
Enable Firewall	Select this to activate the firewall. The ZyXEL Device controls access and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	Select this if you want to let some traffic from the WAN go directly to a computer in the LAN without passing through the ZyXEL Device. See the appendices for more information about triangle route topology.
Max NAT/Firewall Session Per User	Select the maximum number of NAT rules and firewall rules the ZyXEL Device enforces at one time. The ZyXEL Device automatically allocates memory for the maximum number of rules, regardless of whether or not there is a rule to enforce. This is the same number you enter in **Network > NAT > General**.
Packet Direction	This field displays each direction that packets pass through the ZyXEL Device.
Log	Select the situations in which you want to create log entries for firewall events. **No Log** - do not create any log entries **Log Blocked** - (**LAN to WAN** only) create log entries when packets are blocked **Log Forwarded -** (**WAN to LAN** only) create log entries when packets are forwarded **Log All** - create log entries for every packet
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

12.3.2 Firewall Services Screen

Use this screen to enable service blocking, to set up the date and time service blocking is effective, and to maintain the list of services you want to block. To access this screen, click **Security > Firewall > Services**.

Figure 77 Security > Firewall > Services



Each field is described in the following table.

Table 43 Security > Firewall > Services

LABEL	DESCRIPTION
Service Setup	
Enable Services Blocking	Select this to activate service blocking. The **Schedule to** Block section controls what days and what times service blocking is actually effective, however.
Available Services	This is a list of pre-defined services (destination ports) you may prohibit your LAN computers from using. Select the port you want to block, and click **Add** to add the port to the **Blocked Services** field. A custom port is a service that is not available in the pre-defined **Available Services** list. You must define it using the **Type** and **Port Number** fields. See Appendix F on page 249 for some examples of services.
Blocked Services	This is a list of services (ports) that are inaccessible to computers on your LAN when service blocking is effective. To remove a service from this list, select the service, and click **Delete**.
Type	Select **TCP** or **UDP**, based on which one the custom port uses.
Port Number	Enter the range of port numbers that defines the service. For example, suppose you want to define the Gnutella service. Select **TCP** type and enter a port range of **6345-6349**.
Add	Click this to add the selected service in **Available Services** to the **Blocked Services** list.
Delete	Select a service in the **Blocked Services**, and click this to remove the service from the list.

Table 43 Security > Firewall > Services

LABEL	DESCRIPTION
Clear All	Click this to remove all the services in the **Blocked Services** list.
Schedule to Block	
Day to Block	Select which days of the week you want the service blocking to be effective.
Time of Day to Block	Select what time each day you want service blocking to be effective. Enter times in 24-hour format; for example, 3:00pm should be entered as 15:00.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

CHAPTER 13
Phone Book

Use these screens to maintain call-forwarding rules and speed-dial settings.

13.1 Phone Book Overview

Speed dial provides shortcuts for dialing frequently used (VoIP) phone numbers. It is also required if you want to make peer-to-peer calls. In peer-to-peer calls, you call another VoIP device directly without going through a SIP server. In the ZyXEL Device, you must set up a speed dial entry in the phone book in order to do this. Select **Non-Proxy (Use IP or URL)** in the **Type** column and enter the callee's IP address or domain name. The ZyXEL Device sends SIP INVITE requests to the peer VoIP device when you use the speed dial entry.

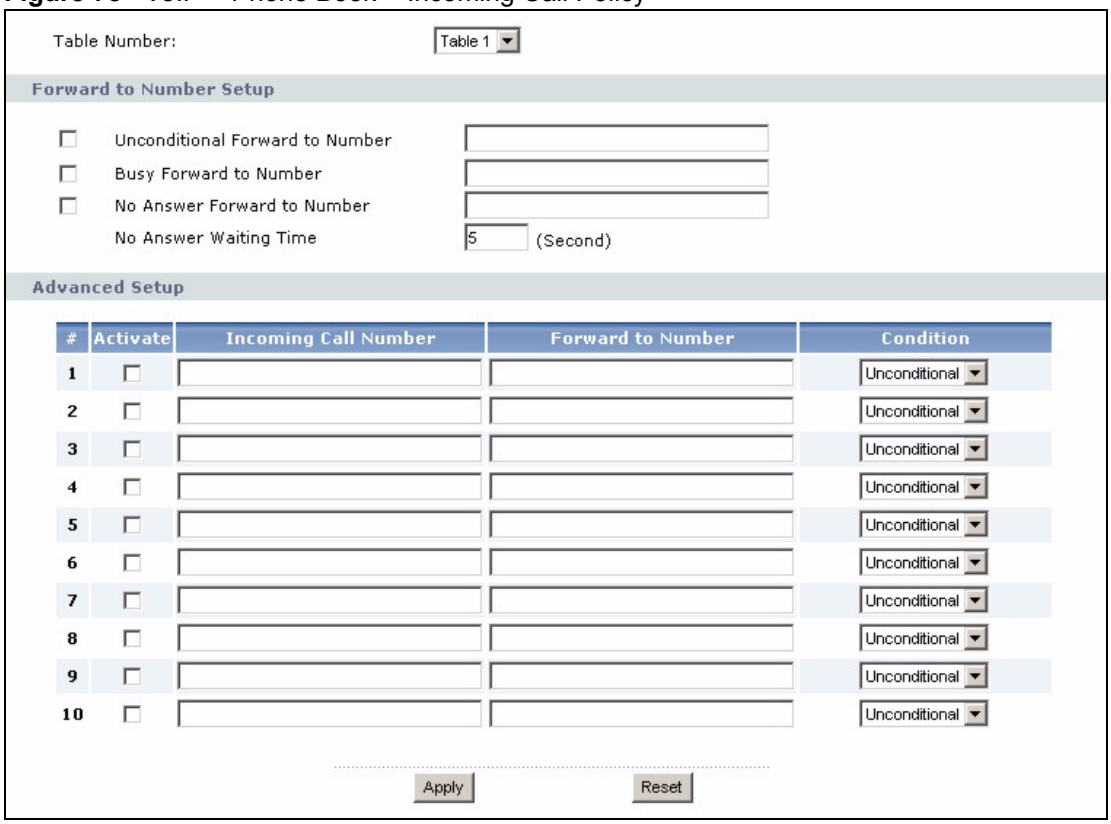
You do not need to configure a SIP account in order to make a peer-to-peer VoIP call.

13.2 Phone Book Screens

13.2.1 Incoming Call Policy Screen

Use this screen to maintain rules for handling incoming calls. You can block, redirect, or accept them. To access this screen, click **VoIP > Phone Book > Incoming Call Policy**.

Figure 78 VoIP > Phone Book > Incoming Call Policy



You can create two sets of call-forwarding rules. Each one is stored in a call-forwarding table. Each field is described in the following table.

Table 44 VoIP > Phone Book > Incoming Call Policy

LABEL	DESCRIPTION
Table Number	Select the call-forwarding table you want to see in this screen. If you change this field, the screen automatically refreshes.
Forward to Number Setup	The ZyXEL Device checks these rules, in the order in which they appear, after it checks the rules in the **Advanced Setup** section.
Unconditional Forward to Number	Select this if you want the ZyXEL Device to forward all incoming calls to the specified phone number, regardless of other rules in the **Forward to Number** section. Specify the phone number in the field on the right.
Busy Forward to Number	Select this if you want the ZyXEL Device to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
No Answer Forward to Number	Select this if you want the ZyXEL Device to forward incoming calls to the specified phone number if the call is unanswered. (See **No Answer Waiting Time**.) Specify the phone number in the field on the right.
No Answer Waiting Time	This field is used by the **No Answer Forward to Number** feature and **No Answer** conditions below. Enter the number of seconds the ZyXEL Device should wait for you to answer an incoming call before it considers the call is unanswered.

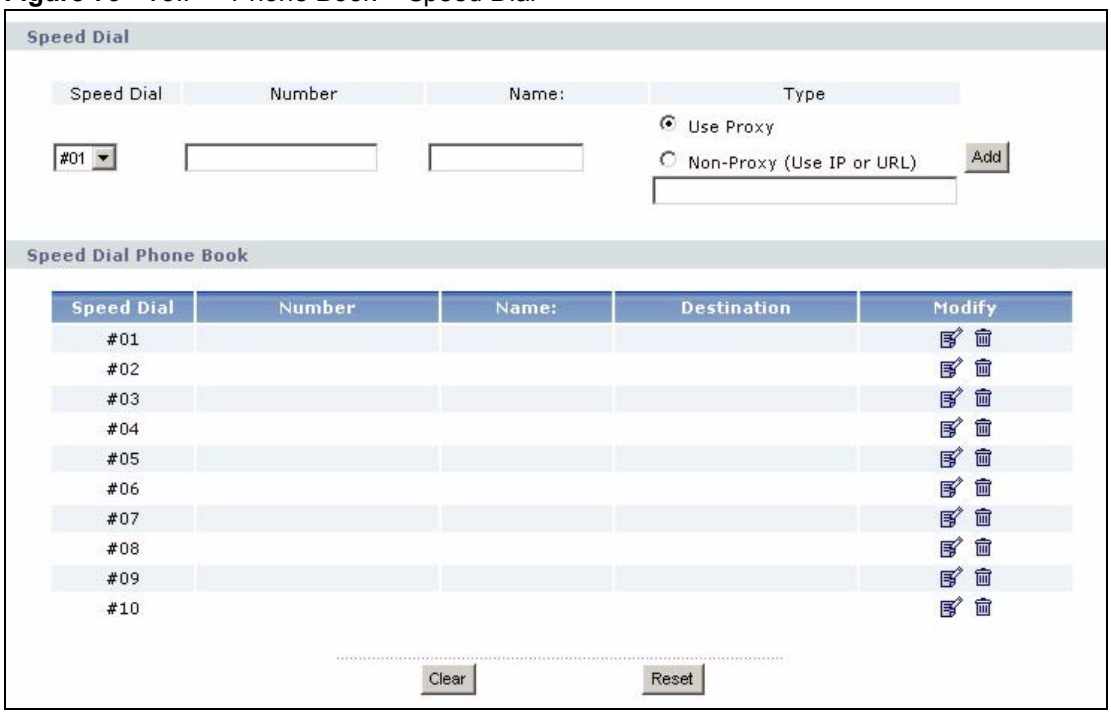
Table 44 VoIP > Phone Book > Incoming Call Policy

LABEL	DESCRIPTION
Advanced Setup	The ZyXEL Device checks these rules before it checks the rules in the **Forward to Number** section.
#	This field is a sequential value, and it is not associated with a specific rule. The sequence is important, however. The ZyXEL Device checks each rule in order, and it only follows the first one that applies.
Activate	Select this to enable this rule. Clear this to disable this rule.
Incoming Call Number	Enter the phone number to which this rule applies.
Forward to Number	Enter the phone number to which you want to forward incoming calls from the **Incoming Call Number**. You may leave this field blank, depending on the **Condition**.
Condition	Select the situations in which you want to forward incoming calls from the **Incoming Call Number**, or select an alternative action. **Unconditional** - The ZyXEL Device immediately forwards any calls from the **Incoming Call Number** to the **Forward to Number**. **Busy -** The ZyXEL Device forwards any calls from the **Incoming Call Number** to the **Forward to Number** when your SIP account already has a call connected. **No Answer -** The ZyXEL Device forwards any calls from the **Incoming Call Number** to the **Forward to Number** when the call is unanswered. (See **No Answer Waiting Time**.) **Block -** The ZyXEL Device rejects calls from the **Incoming Call Number**. **Accept -** The ZyXEL Device allows calls from the **Incoming Call Number**. You might create a rule with this condition if you do not want incoming calls from someone to be forwarded by rules in the **Forward to Number** section.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its last-saved value.

13.2.2 Speed Dial Screen

You have to create speed-dial entries if you want to make peer-to-peer calls or call SIP numbers that use letters. You can also create speed-dial entries for frequently-used SIP phone numbers. Use this screen to add, edit, or remove speed-dial entries. To access this screen, click **VoIP > Phone Book > Speed Dial**.

Figure 79 VoIP > Phone Book > Speed Dial



Each field is described in the following table.

Table 45 VoIP > Phone Book > Speed Dial

LABEL	DESCRIPTION
Speed Dial	Use this section to create or edit speed-dial entries.
Speed Dial	Select the speed-dial number you want to use for this phone number.
Number	Enter the SIP number you want the ZyXEL Device to call when you dial the speed-dial number.
Name	Enter a name to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.
Type	Select **Use Proxy** if you want to use one of your SIP accounts to call this phone number. Select **Non-Proxy (Use IP or URL)** if you want to use a different SIP server or if you want to make a peer-to-peer call. In this case, enter the IP address or domain name of the SIP server or the other party in the field below.
Add	Click this to use the information in the **Speed Dial** section to update the **Speed Dial Phone Book** section.
Speed Dial Phone Book	Use this section to look at all the speed-dial entries and to erase them.
Speed Dial	This field displays the speed-dial number you should dial to use this entry. You should dial the numbers the way they appear in the screen.
Number	This field displays the SIP number the ZyXEL Device calls when you dial the speed-dial number.
Name	This field displays the name of the party you call when you dial the speed-dial number.

Table 45 VoIP > Phone Book > Speed Dial

LABEL	DESCRIPTION
Destination	This field is blank, if the speed-dial entry uses one of your SIP accounts. Otherwise, this field shows the IP address or domain name of the SIP server or other party. (This field corresponds with the **Type** field in the **Speed Dial** section.)
Modify	Use this field to edit or erase the speed-dial entry. Click the **Edit** icon to copy the information for this speed-dial entry into the **Speed Dial** section, where you can change it. Click the **Remove** icon to erase this speed-dial entry.
Clear	Click this to erase all the speed-dial entries.
Reset	Click this to set every field in this screen to its last-saved value.

CHAPTER 14
Content Filter

Use these screens to create and enforce policies that restrict access to the Internet based on content.

14.1 Content Filtering Overview

Internet content filtering allows you to create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain web features or specific URL keywords.

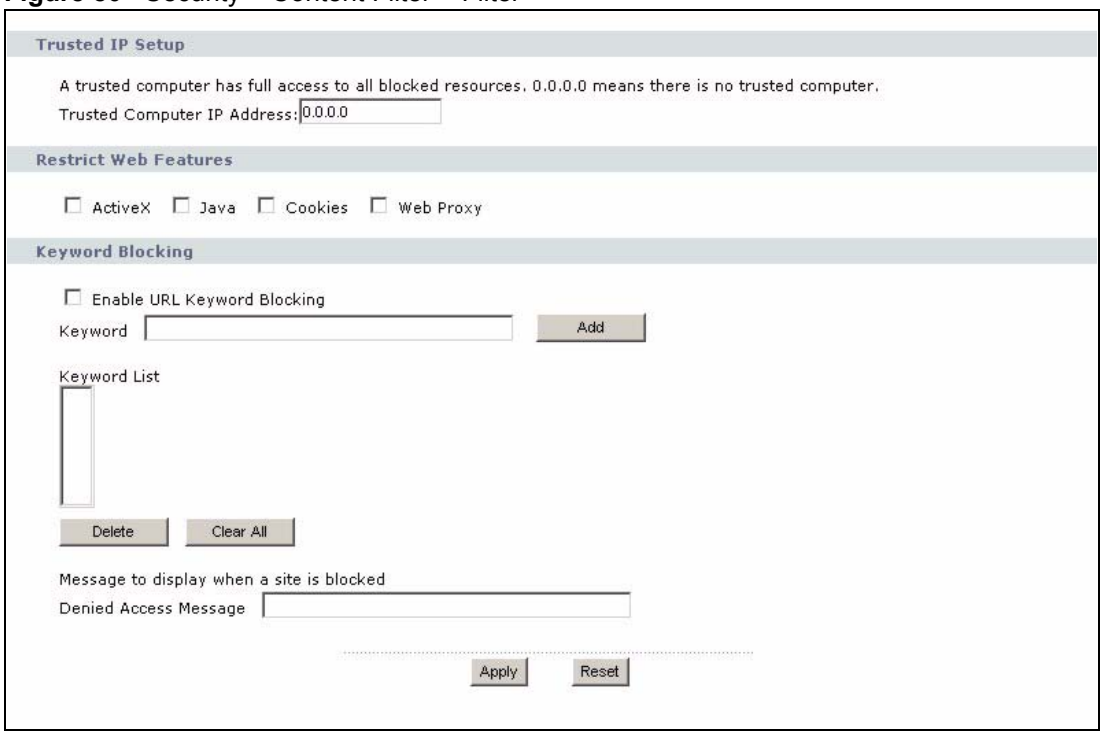
The ZyXEL Device can block web features such as ActiveX controls, Java applets, cookies and disable web proxies. The ZyXEL Device also allows you to define time periods and days during which the ZyXEL Device performs content filtering.

14.2 Content Filtering Screens

14.2.1 Content Filter Screen

Use this screen to set up a trusted IP address, which web features are restricted, and which keywords are blocked when content filtering is effective. To access this screen, click **Security > Content Filter > Filter**.

Figure 80 Security > Content Filter > Filter



Each field is described in the following table.

Table 46 Security > Content Filter > Filter

LABEL	DESCRIPTION
Trusted IP Setup	
Trusted Computer IP Address	You can allow a specific computer to access all Internet resources without the restrictions you set in these screens. Enter the IP address of the trusted computer.
Restrict Web Features	Select the web features you want to disable. If a user downloads a page with a restricted feature, that part of the web page appears blank or grayed out. **ActiveX** - This is a tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again. **Java** - This is used to build downloadable Web components or Internet and intranet business applications of all kinds. **Cookies** - This is used by Web servers to track usage and to provide service based on ID. **Web Proxy** - This is a server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN, it is possible for LAN users to avoid content filtering restrictions.
Keyword Blocking	
Enable URL Keyword Blocking	Select this if you want the ZyXEL Device to block Web sites based on words in the web site address. For example, if you block the keyword **bad**, http://www.website.com/bad.html is blocked.
Keyword	Type a keyword you want to block in this field. You can use up to 64 printable ASCII characters. There is no wildcard character, however.

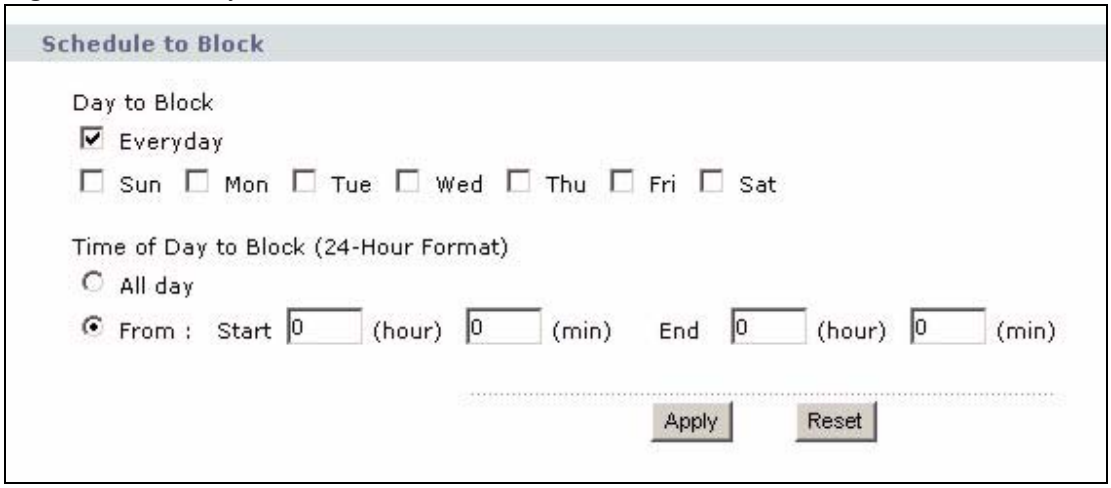
Table 46 Security > Content Filter > Filter

LABEL	DESCRIPTION
Add	Click this to add the specified **Keyword** to the **Keyword List**. You can enter up to 64 keywords.
Keyword List	This field displays the keywords that are blocked when **Enable URL Keyword Blocking** is selected. To delete a keyword, select it, click **Delete**, and click **Apply**.
Delete	Click **Delete** to remove the selected keyword in the **Keyword List**. The keyword disappears after you click **Apply**.
Clear All	Click this button to remove all of the keywords in the **Keyword List**.
Denied Access Message	Enter the message that is displayed when the ZyXEL Device's content filter feature blocks access to a web site.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

14.2.2 Content Filter Schedule Screen

Use this screen to set up the schedule when content filtering is effective. To access this screen, click **Security > Content Filter > Schedule**.

Figure 81 Security > Content Filter > Schedule



Each field is described in the following table.

Table 47 Security > Content Filter > Schedule

LABEL	DESCRIPTION
Day to Block	Select which days of the week you want content filtering to be effective.
Time of Day to Block	Select what time each day you want content filtering to be effective. Enter times in 24-hour format; for example, 3:00pm should be entered as 15:00.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

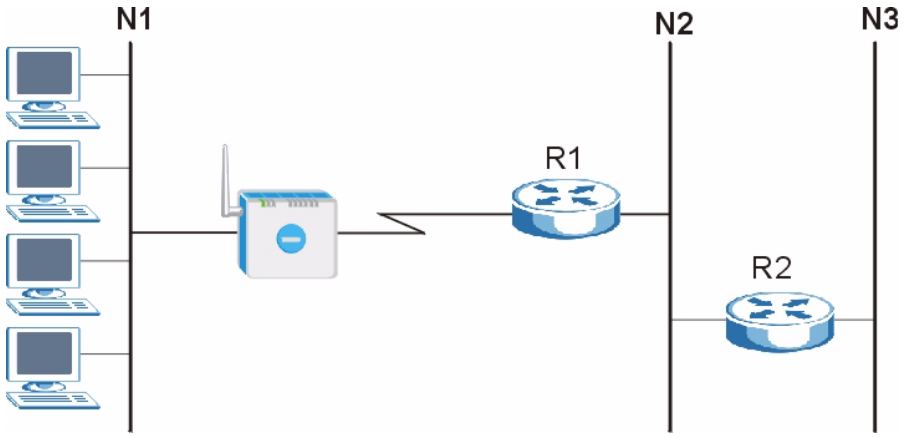
CHAPTER 15
Static Route

Use these screens to configure static routes on the ZyXEL Device.

15.1 Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the ZyXEL Device has no knowledge of the networks beyond. For instance, the ZyXEL Device knows about network N2 in the following figure through remote node Router 1. However, the ZyXEL Device is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the ZyXEL Device about the networks beyond the remote nodes.

Figure 82 Example of Static Routing Topology



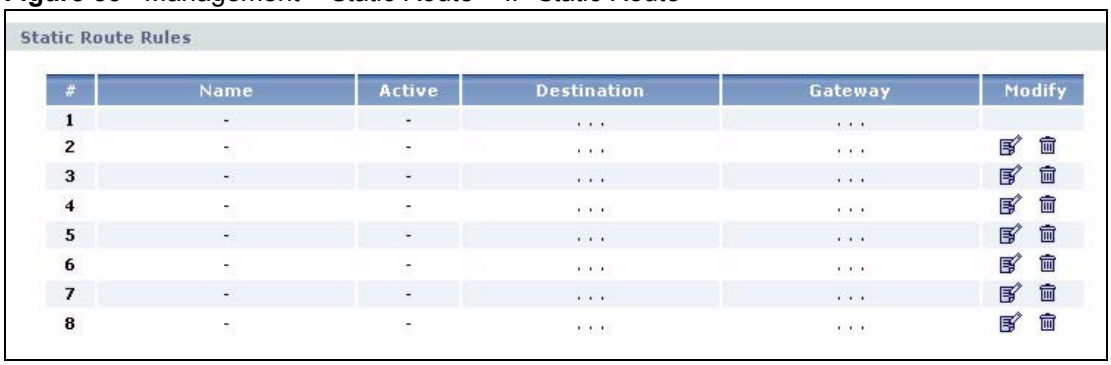
15.2 Static Route Screens

15.2.1 IP Static Route Screen

Use this screen to look at static routes in the ZyXEL Device. To access this screen, click **Management > Static Route > IP Static Route**.

Note: The first static route is the default route and cannot be modified or deleted.

Figure 83 Management > Static Route > IP Static Route



Each field is described in the following table.

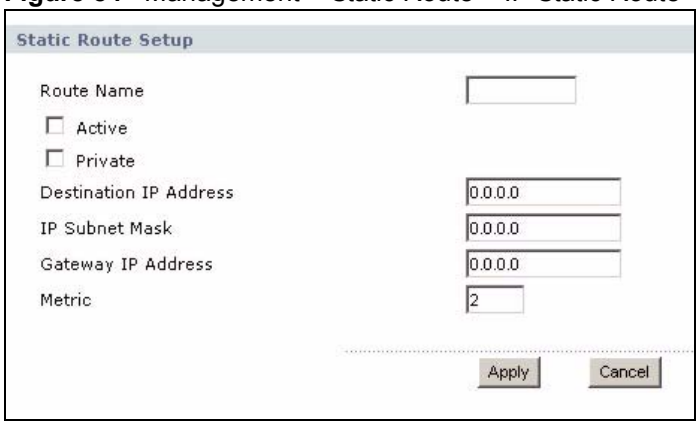
Table 48 Management > Static Route > IP Static Route

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific rule. The sequence is important, however. The ZyXEL Device checks each rule in order, and it follows only the first one that applies.
Name	This field displays the name that describes the static route.
Active	This field shows whether this static route is active (**Yes**) or not (**No**).
Destination	This field displays the destination IP address(es) that this static route affects.
Gateway	This field displays the IP address of the gateway to which the ZyXEL Device should send packets for the specified **Destination**. The gateway is a router or a switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Modify	Use this field to edit or erase the static route. Click the **Edit** icon to open the **IP Static Route Edit** screen for this static route. Click the **Remove** icon to erase this static route.

15.2.2 IP Static Route Edit Screen

Use this screen to edit a static route in the ZyXEL Device. To access this screen, click an **Edit** icon in **Management > Static Route > IP Static Route**.

Figure 84 Management > Static Route > IP Static Route > Edit



Each field is described in the following table.

Table 49 Management > Static Route > IP Static Route > Edit

LABEL	DESCRIPTION
Route Name	Enter the name of the static route.
Active	Select this if you want the static route to be used. Clear this if you do not want the static route to be used.
Private	Select this if you do not want the ZyXEL Device to tell other routers about this static route. For example, you might select this if the static route is in your LAN. Clear this if you want the ZyXEL Device to tell other routers about this static route.
Destination IP Address	Enter one of the destination IP addresses that this static route affects.
IP Subnet Mask	Enter the subnet mask that defines the range of destination IP addresses that this static route affects. If this static route affects only one IP address, enter 255.255.255.255.
Gateway IP Address	Enter the IP address of the gateway to which the ZyXEL Device should send packets for the specified **Destination**. The gateway is a router or a switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	Usually, you should keep the default value. This field is related to RIP. See Chapter 8 on page 83 for more information. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the metric, the lower the "cost". RIP uses hop count as the measurement of cost, where 1 is for a directly-connected network. The metric must be 1-15; if you use a value higher than 15, the routers assume the link is down.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to return to the previous screen without saving your changes.

CHAPTER 16
Remote MGMT

Use these screens to control which computers can use which services to access the ZyXEL Device on each interface.

16.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyXEL Device interface (if any) from which computers.

You may manage your ZyXEL Device from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (LAN and WAN)
- Neither (Disable).

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

You may only have one remote management session running at a time. The ZyXEL Device automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1. Telnet
2. HTTP

16.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in one of the remote management screens.
3. The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.
4. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

16.1.2 Remote Management and NAT

When NAT is enabled:

- Use the ZyXEL Device's WAN IP address when configuring from the WAN.
- Use the ZyXEL Device's LAN IP address when configuring from the LAN.

16.1.3 System Timeout

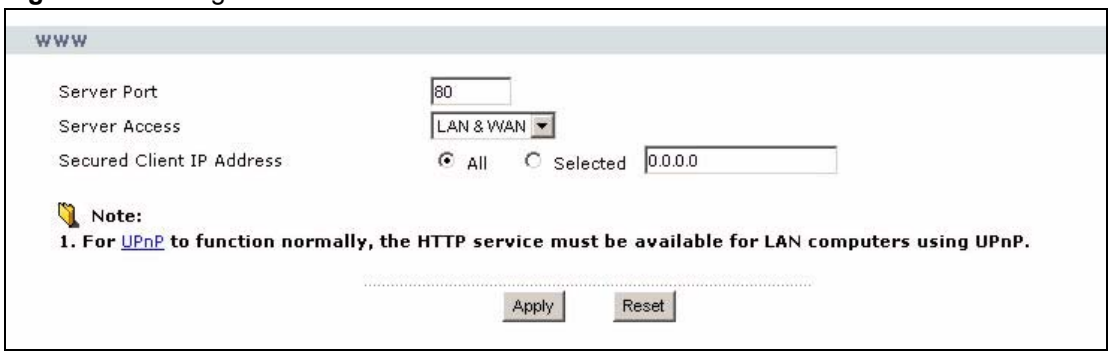
There is a default system management idle timeout of five minutes (three hundred seconds). The ZyXEL Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **Maintenance > System > General** screen.

16.2 Remote Management Screens

16.2.1 WWW Screen

Use this screen to control HTTP access to your ZyXEL Device. To access this screen, click **Management > Remote MGMT > WWW**.

Figure 85 Management > Remote MGMT > WWW



Each field is described in the following table.

Table 50 Management > Remote MGMT > WWW

LABEL	DESCRIPTION
Server Port	Enter the port number this service can use to access the ZyXEL Device. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	Select **All** to allow any computer to access the ZyXEL Device using this service. Select **Selected** to only allow the computer with the IP address that you specify to access the ZyXEL Device using this service.

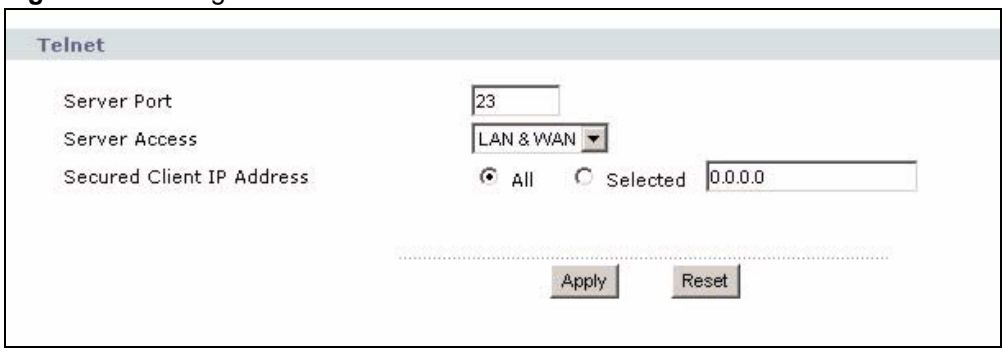
Table 50 Management > Remote MGMT > WWW

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its default value.

16.2.2 Telnet Screen

Use this screen to control Telnet access to your ZyXEL Device. To access this screen, click **Management > Remote MGMT > Telnet**.

Figure 86 Management > Remote MGMT > Telnet



Each field is described in the following table.

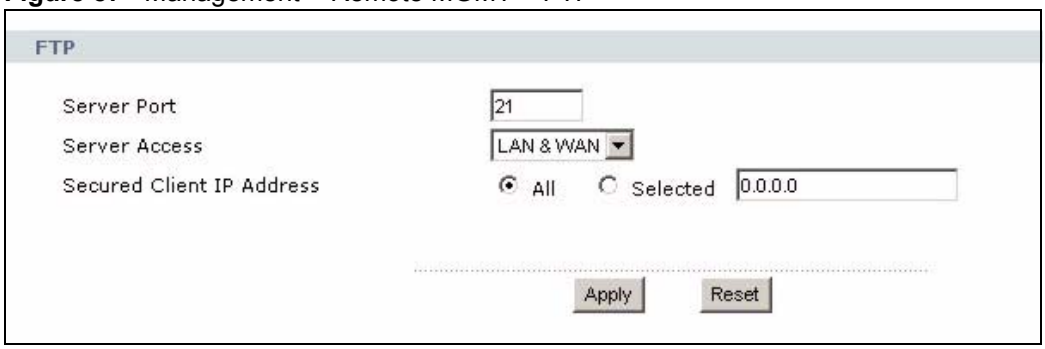
Table 51 Management > Remote MGMT > Telnet

LABEL	DESCRIPTION
Server Port	Enter the port number this service can use to access the ZyXEL Device. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	Select **All** to allow any computer to access the ZyXEL Device using this service. Select **Selected** to only allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its default value.

16.2.3 FTP Screen

Use this screen to control FTP access to your ZyXEL Device. To access this screen, click **Management > Remote MGMT > FTP**.

Figure 87 Management > Remote MGMT > FTP



Each field is described in the following table.

Table 52 Management > Remote MGMT > FTP

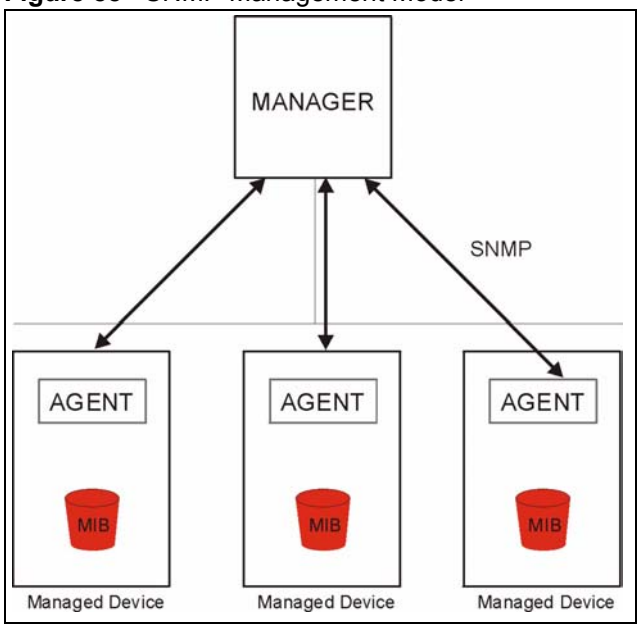
LABEL	DESCRIPTION
Server Port	Enter the port number this service can use to access the ZyXEL Device. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	Select **All** to allow any computer to access the ZyXEL Device using this service. Select **Selected** to only allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its default value.

16.3 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation.

Note: SNMP is only available if TCP/IP is configured.

Figure 88 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyXEL Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

16.3.1 Supported MIBs

The ZyXEL Device supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

16.3.2 SNMP Traps

The ZyXEL Device will send traps to the SNMP manager when any one of the following events occurs:

Table 53 SNMP Traps

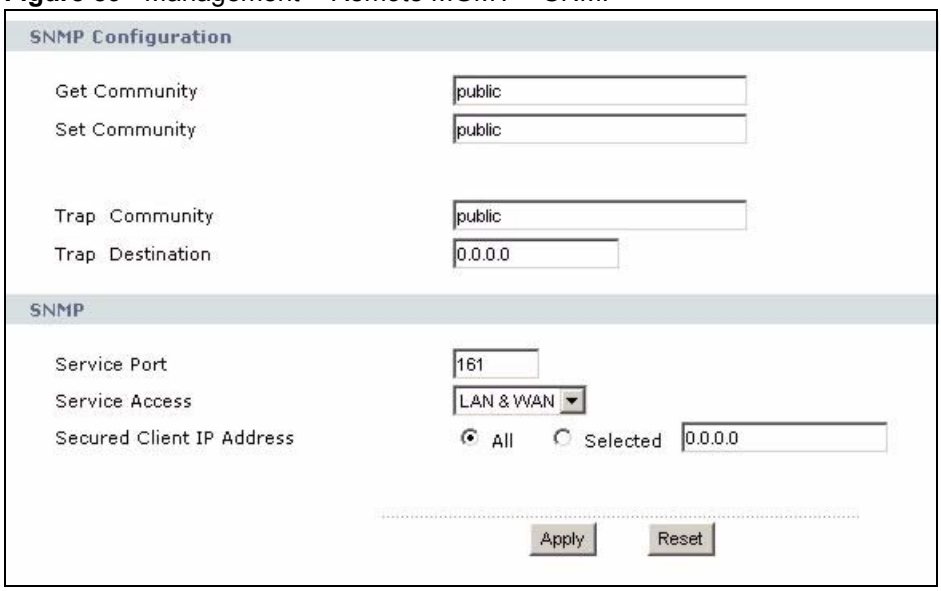
TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in *RFC-1215*)	A trap is sent after booting (power on).
1	warmStart (defined in *RFC-1215*)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in *RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot:	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

16.3.3 Configuring SNMP

To change your ZyXEL Device's SNMP settings, click **Advanced > Remote MGMT** > **SNMP**. The screen appears as shown.

Use this screen to control FTP access to your ZyXEL Device. To access this screen, click **Management > Remote MGMT > SNMP**.

Figure 89 Management > Remote MGMT > SNMP



The following table describes the labels in this screen.

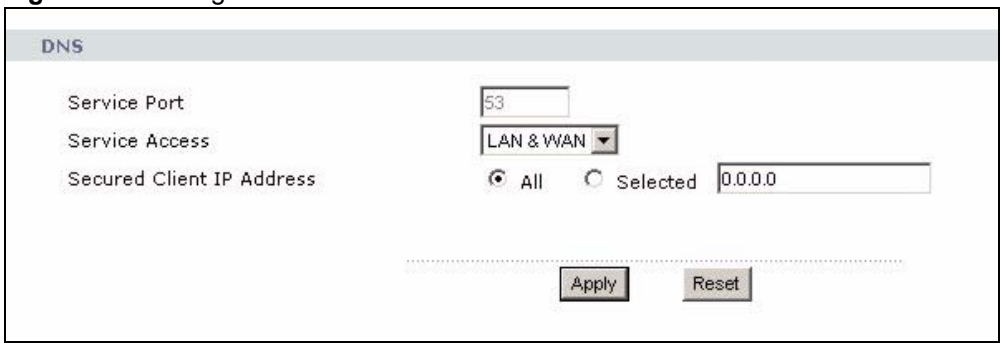
Table 54 Remote Management: SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap Community	Enter the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Trap Destination	Enter the IP address of the station to send your SNMP traps to.
SNMP	
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click this button to save your customized settings and exit this screen.
Reset	Click this button to set each field in this screen to its default value.

16.3.4 DNS Screen

Use this screen to control DNS access to your ZyXEL Device. To access this screen, click **Management > Remote MGMT > DNS**.

Figure 90 Management > Remote MGMT > DNS



Each field is described in the following table.

Table 55 Management > Remote MGMT > DNS

LABEL	DESCRIPTION
Server Port	This field is read-only. This field displays the port number this service uses to access the ZyXEL Device. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	Select **All** to allow any computer to access the ZyXEL Device using this service. Select **Selected** to only allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

16.3.5 Security Screen

Use this screen to control how your ZyXEL Device responds to other types of requests. To access this screen, click **Management > Remote MGMT > Security**.

Figure 91 Management > Remote MGMT > Security

Each field is described in the following table.

Table 56 Management > Remote MGMT > Security

LABEL	DESCRIPTION
Respond to Ping on	Select the interface(s) on which the ZyXEL Device should respond to incoming ping requests. **Disable** - the ZyXEL Device does not respond to any ping requests. **LAN** - the ZyXEL Device only responds to ping requests received from the LAN. **WAN** - the ZyXEL Device only responds to ping requests received from the WAN. **LAN & WAN** - the ZyXEL Device responds to ping requests received from the LAN or the WAN.
Do not respond to requests for unauthorized services	Select this to prevent outsiders from discovering your ZyXEL Device by sending requests to unsupported port numbers. If an outside user attempts to probe an unsupported port on your ZyXEL Device, an ICMP response packet is automatically returned. This allows the outside user to know the ZyXEL Device exists. Your ZyXEL Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed. If you clear this, your ZyXEL Device replies with an ICMP Port Unreachable packet for a port probe on unused UDP ports and with a TCP Reset packet for a port probe on unused TCP ports.
Apply	Click this to save your changes.
Cancel	Click this to set every field in this screen to its default value.

CHAPTER 17
UPnP

Use this screen to set up UPnP.

17.1 Introducing Universal Plug and Play

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

17.1.1 How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

17.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See Chapter 9 on page 97 for further information about NAT.

17.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

17.1.4 UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementors Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

The ZyXEL Device only sends UPnP multicasts to the LAN.

See later sections for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

17.2 UPnP Examples

17.2.1 Installing UPnP in Windows Example

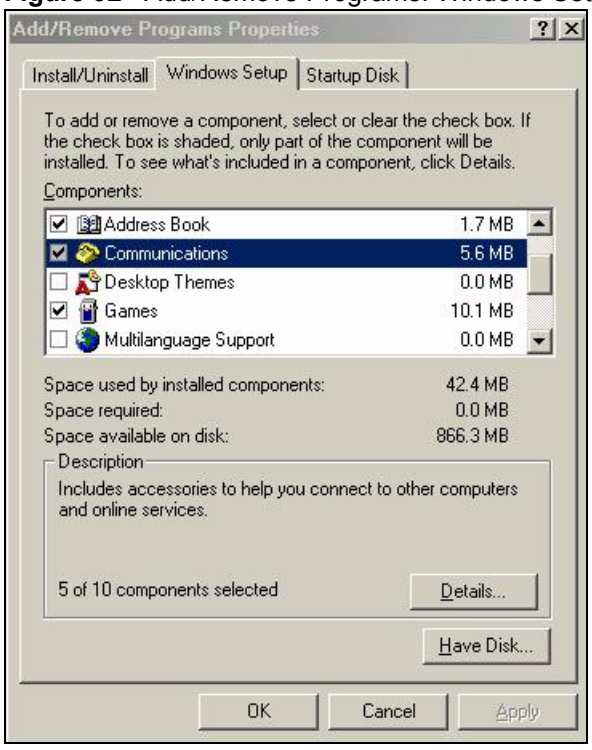
This section shows how to install UPnP in Windows Me and Windows XP.

17.2.1.1 Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

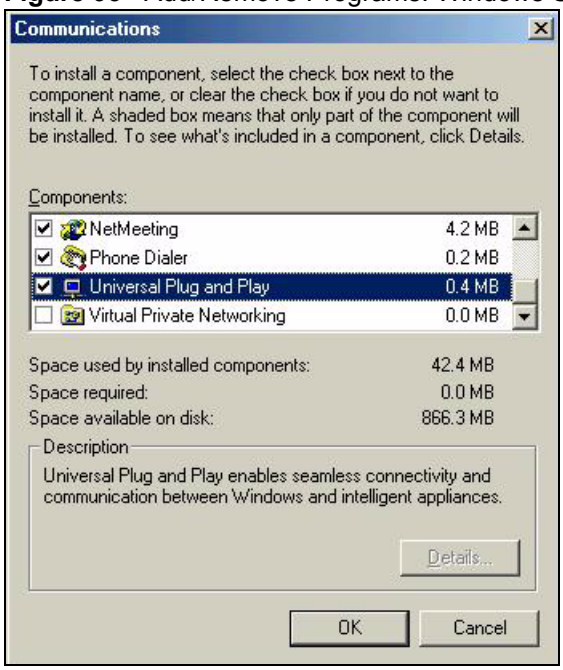
1. Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
2. Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 92 Add/Remove Programs: Windows Setup: Communication


Add/Remove Programs Properties
Install/Uninstall
Windows Setup
Startup Disk
To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.
Components:
Address Book 1.7 MB
Communications 5.6 MB
Desktop Themes 0.0 MB
Games 10.1 MB
Multilanguage Support 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Includes accessories to help you connect to other computers and online services.
5 of 10 components selected
Details...
Have Disk...
OK
Cancel
Apply

3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Figure 93 Add/Remove Programs: Windows Setup: Communication Components


Communications
To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
NetMeeting 4.2 MB
Phone Dialer 0.2 MB
Universal Plug and Play 0.4 MB
Virtual Private Networking 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.
Details...
OK
Cancel

4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

17.2.1.2 Installing UPnP in Windows XP

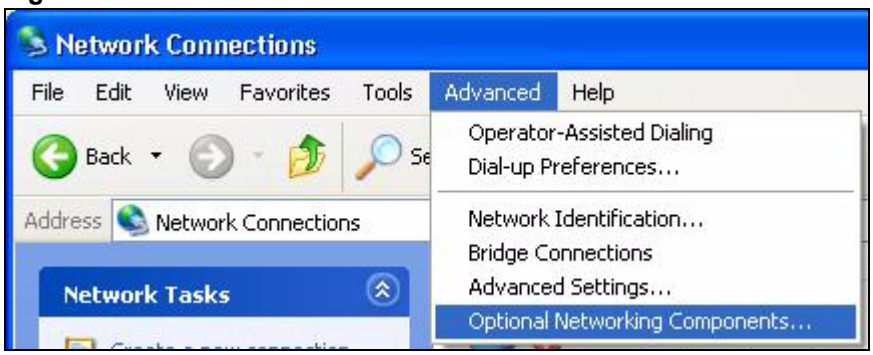
Follow the steps below to install the UPnP in Windows XP.

1 Click **Start** and **Control Panel**.

2 Double-click **Network Connections**.

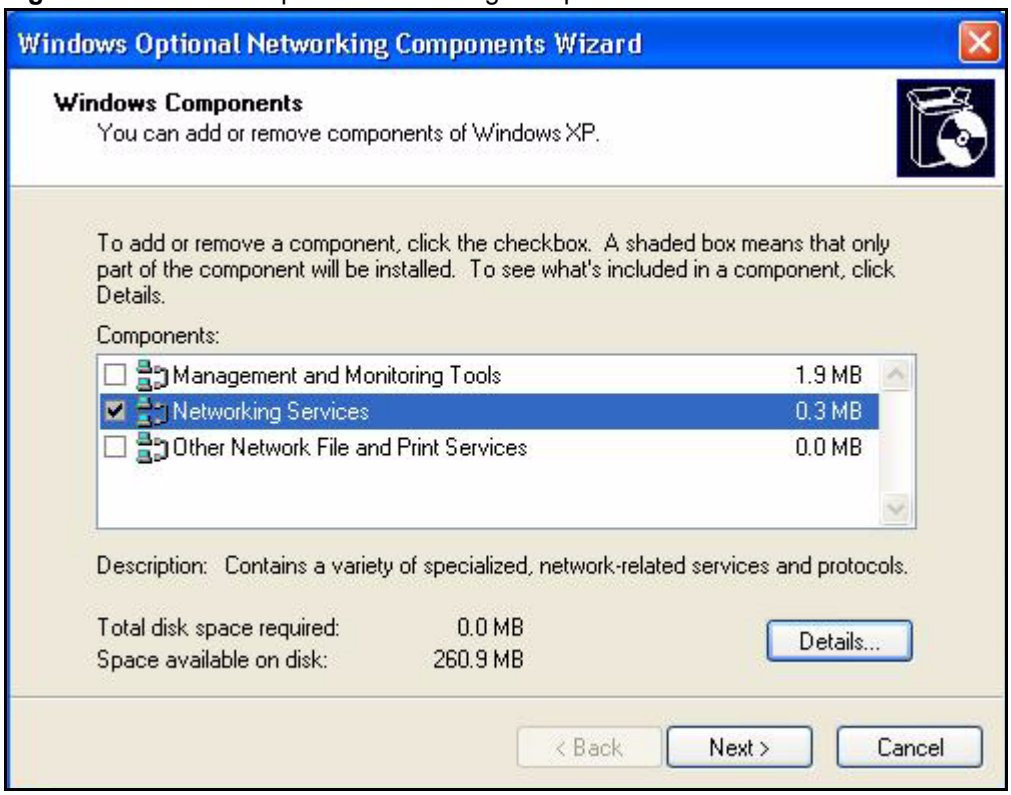
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.

Figure 94 Network Connections



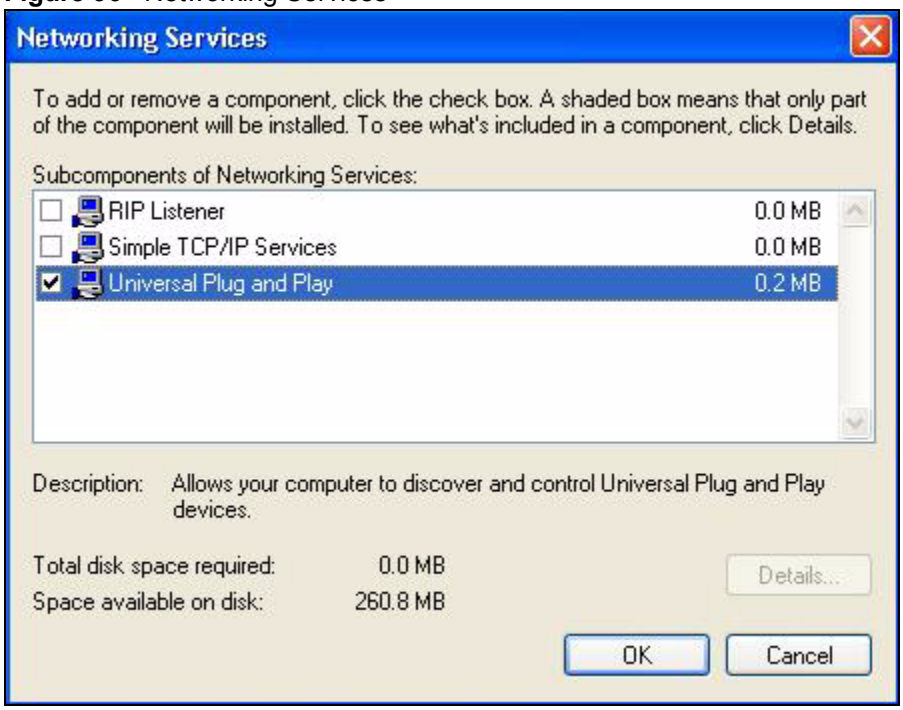
4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 95 Windows Optional Networking Components Wizard


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 1.9 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 260.9 MB
Details...
< Back
Next >
Cancel

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 96 Networking Services


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
Universal Plug and Play 0.2 MB
Description: Allows your computer to discover and control Universal Plug and Play devices.
Total disk space required: 0.0 MB
Space available on disk: 260.8 MB
Details...
OK
Cancel

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

17.2.2 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL Device.

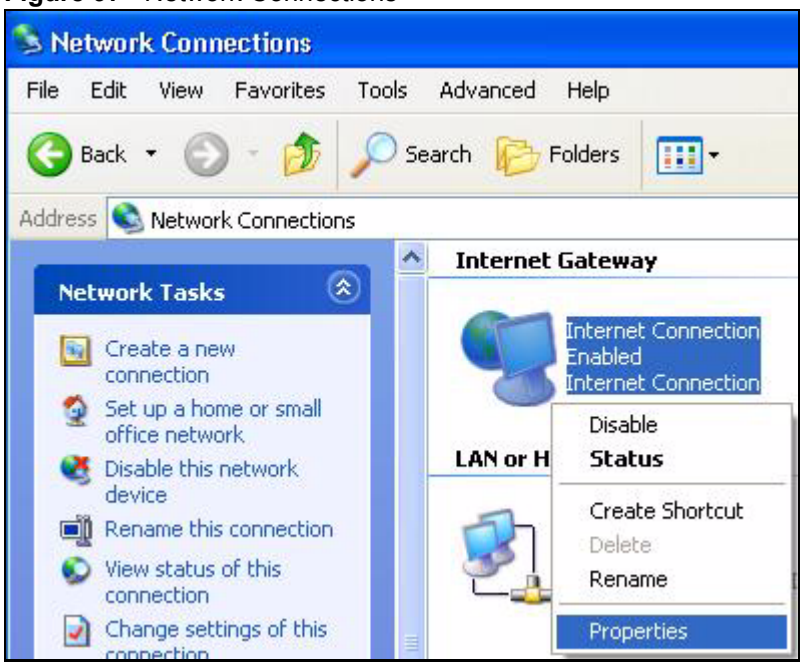
Make sure the computer is connected to a LAN port of the ZyXEL Device. Turn on your computer and the ZyXEL Device.

17.2.2.1 Auto-discover Your UPnP-enabled Network Device

1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

2 Right-click the icon and select **Properties**.

Figure 97 Network Connections



3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 98 Internet Connection Properties

Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 99 Internet Connection Properties: Advanced Settings

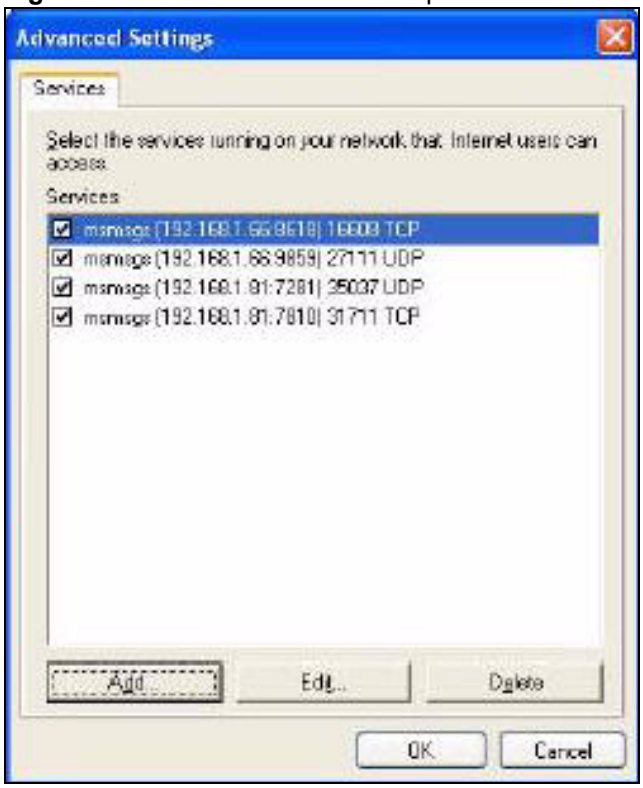
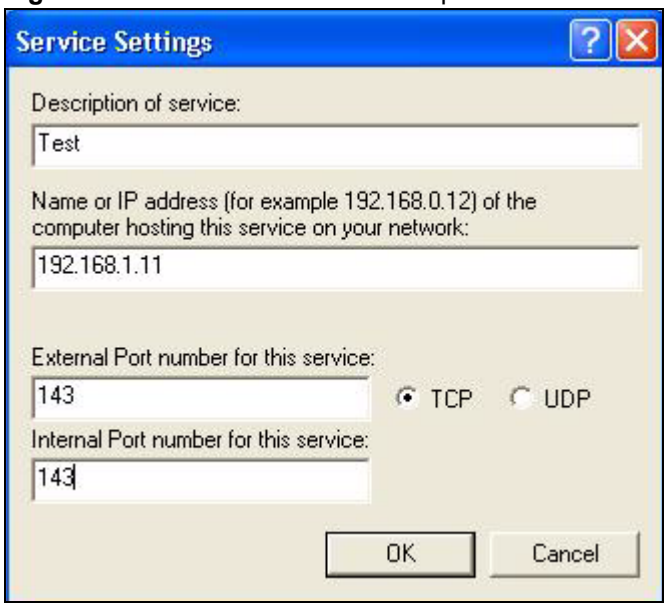


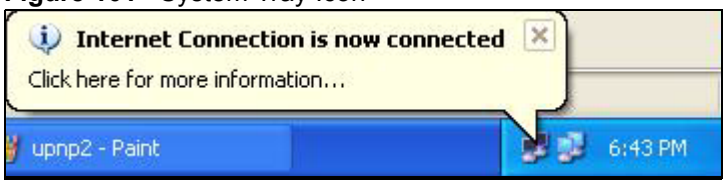
Figure 100 Internet Connection Properties: Advanced Settings: Add



5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 101 System Tray Icon



7 Double-click on the icon to display your current Internet connection status.

Figure 102 Internet Connection Status

17.2.2.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the ZyXEL Device without finding out the IP address of the ZyXEL Device first. This becomes helpful if you do not know the IP address of the ZyXEL Device.

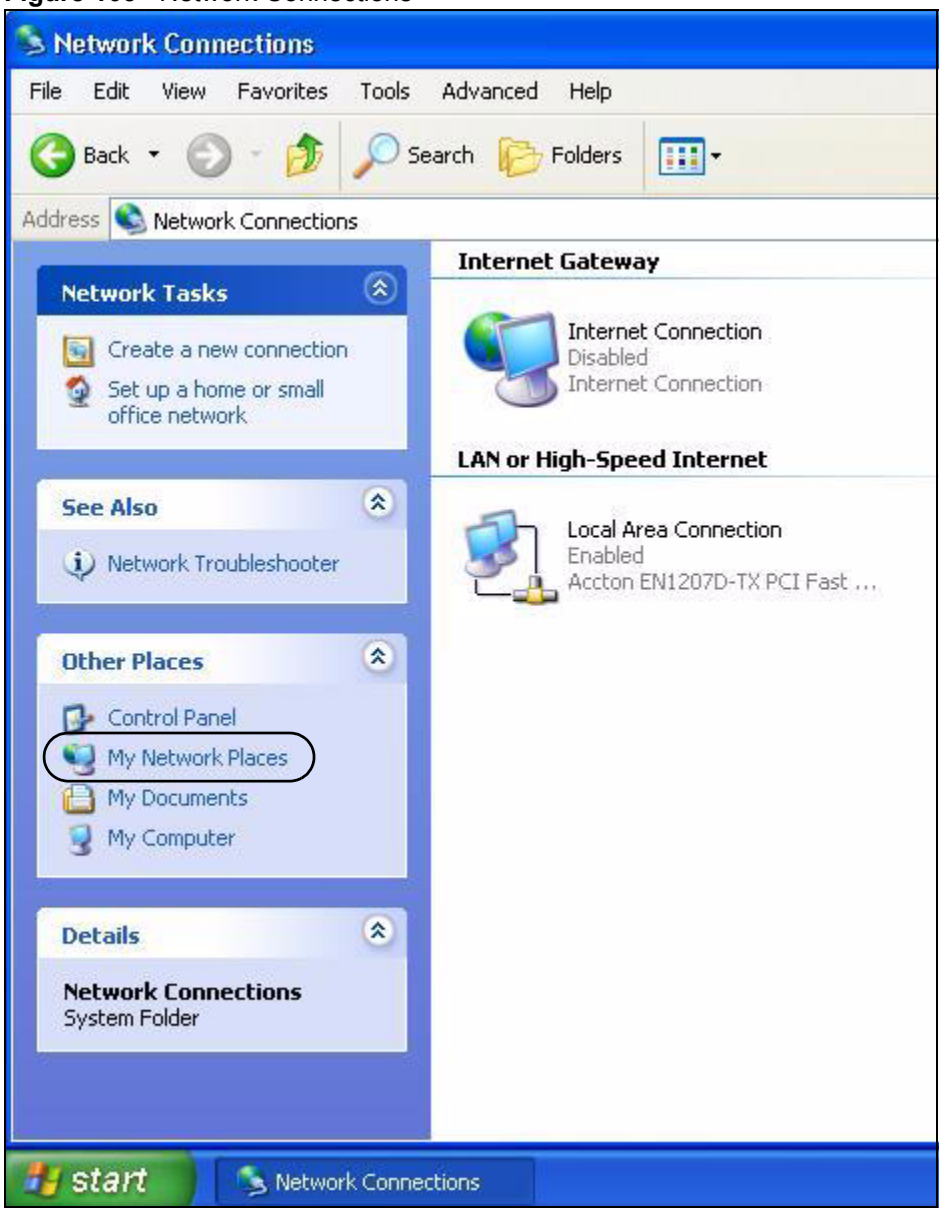
Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

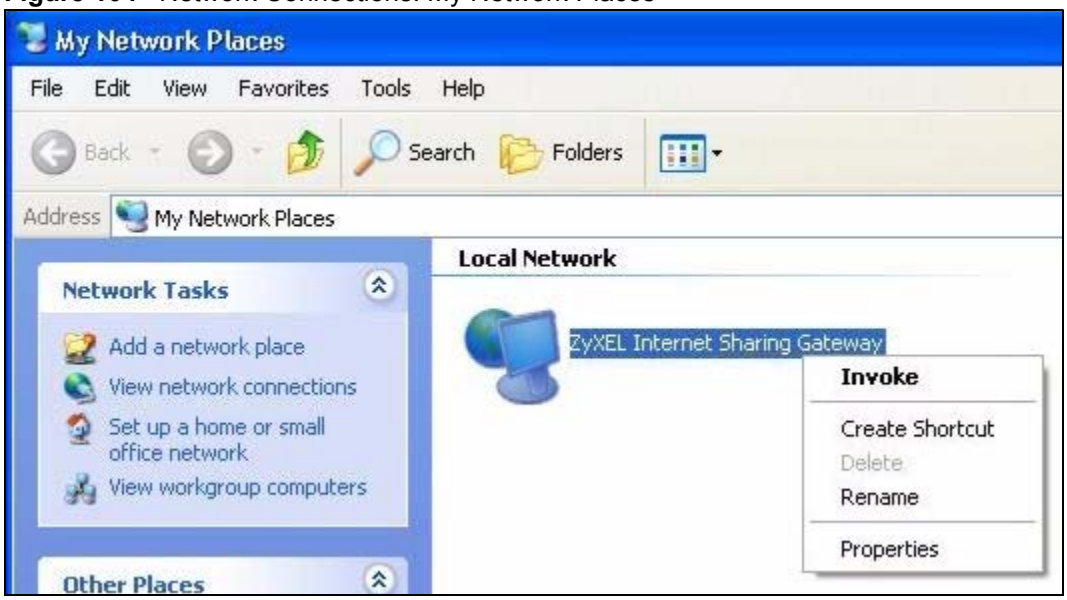
Figure 103 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your ZyXEL Device and select **Invoke**. The web configurator login screen displays.

Figure 104 Network Connections: My Network Places



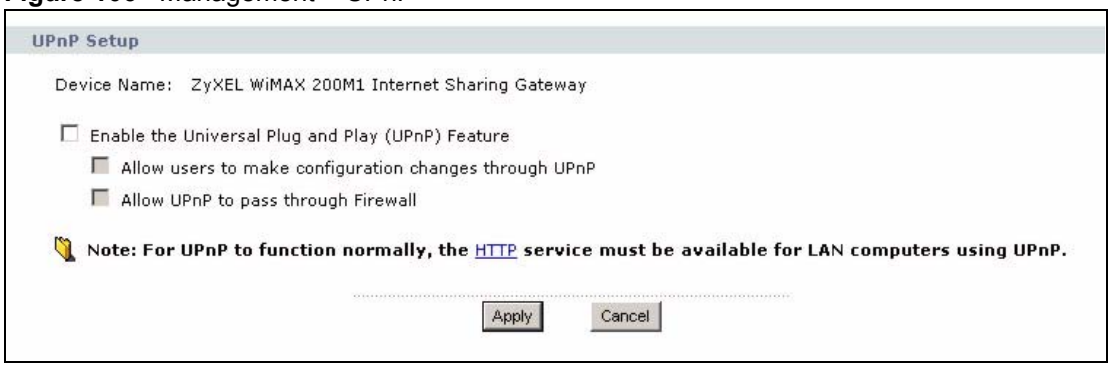
6 Right-click on the icon for your ZyXEL Device and select **Properties**. A properties window displays with basic information about the ZyXEL Device.

Figure 105 Network Connections: My Network Places: Properties: Example

17.3 UPnP Screen

Use this screen to set up UPnP in your ZyXEL Device. To access this screen, click **Management > UPnP**.

Figure 106 Management > UPnP


UPnP Setup
Device Name: ZyXEL WiMAX 200M1 Internet Sharing Gateway
Enable the Universal Plug and Play (UPnP) Feature
Allow users to make configuration changes through UPnP
Allow UPnP to pass through Firewall
Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.
Apply
Cancel

Each field is described in the following table.

Table 57 Management > UPnP

LABEL	DESCRIPTION
Device Name	This field identifies your device in UPnP applications.
Enable the Universal Plug and Play (UPnP) Feature	Select this to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyXEL Device's IP address. You still have to enter the password, however.
Allow users to make configuration changes through UPnP	Select this to allow UPnP-enabled applications to automatically configure the ZyXEL Device so that they can communicate through the ZyXEL Device. For example, using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through Firewall	Select this to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this if you want the firewall to check UPnP application packets (for example, MSN packets).
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its default value.

CHAPTER 18
Logs

Use these screens to look at log entries and alerts and to configure the ZyXEL Device's log and alert settings.

18.1 Logs Overview

For a list of log messages, see Section 18.3 on page 182.

18.1.1 Alerts

An alert is a type of log that warrants more serious attention. Some categories such as **System Errors** consist of both logs and alerts.

18.1.2 Syslog Logs

There are two types of syslog: event logs and traffic logs. The device generates an event log when a system event occurs, for example, when a user logs in or the device is under attack. The device generates a traffic log when a "session" is terminated. A traffic log summarizes the session's type, when it started and stopped the amount of traffic that was sent and received and so on. An external log analyzer can reconstruct and analyze the traffic flowing through the device after collecting the traffic logs.

Table 58 Syslog Logs

LOG MESSAGE	DESCRIPTION
Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"	This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the **Log Settings** screen. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.
Traffic Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="Traffic Log" note="Traffic Log" devID="<mac address>" cat="Traffic Log" duration=seconds sent=sentBytes rcvd=receiveBytes dir="<from:to>" protoID=IPProtocolID proto="serviceName" trans="IPSec/ Normal"	This message is sent by the device when the connection (session) is closed. The facility is defined in the Log Settings screen. The severity is the traffic log type. The message and note always display "Traffic Log". The "proto" field lists the service name. The "dir" field lists the incoming and outgoing interfaces ("LAN:LAN", "LAN:WAN", "LAN:DEV" for example).

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 59 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

18.2 Logs Screens

18.2.1 Log Viewer Screen

Use this screen to look at log entries and alerts. Alerts are written in red. To access this screen, click **Maintenance > Logs > View Log**.

Figure 107 Maintenance > Logs > View Log

Click a column header to sort log entries in descending (later-to-earlier) order. Click again to sort in ascending order. The small triangle next to a column header indicates how the table is currently sorted (pointing downward is descending; pointing upward is ascending). Each field is described in the following table.

Table 60 Maintenance > Logs > View Log

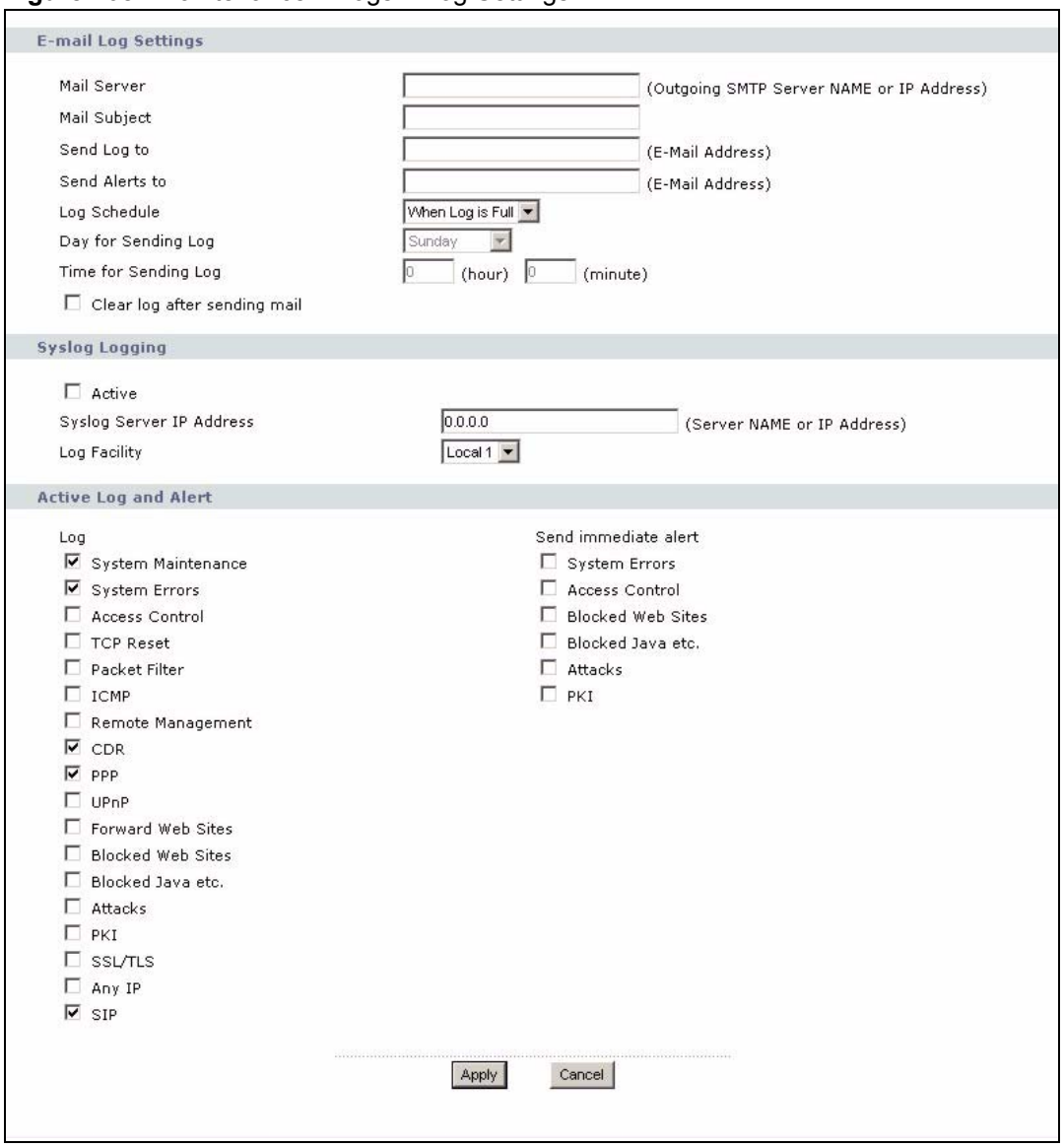
LABEL	DESCRIPTION
Display	Select a category whose log entries you want to view. To view all logs, select **All Logs**. The list of categories depends on what log categories are selected in the **Log Settings** page.
Email Log Now	Click this to send the log screen to the e-mail address specified in the **Log Settings** page.
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to clear all the log entries, regardless of what is shown on the log screen.
#	This field is a sequential value, and it is not associated with a specific log entry.
Time	This field displays the time the log entry was recorded.
Message	This field displays the reason for the log entry. See Section 18.3 on page 182.
Source	This field displays the source IP address and the port number of the incoming packet. In many cases, some or all of this information may not be available.
Destination	This field lists the destination IP address and the port number of the incoming packet. In many cases, some or all of this information may not be available.
Note	This field displays additional information about the log entry.

18.2.2 Log Settings Screen

Use this screen to configure where the ZyXEL Device sends logs and alerts, the schedule for sending logs, and which logs and alerts are sent or recorded.

To access this screen, click **Maintenance > Logs > Log Settings**.

Figure 108 Maintenance > Logs > Log Settings



Each field is described in the following table.

Table 61 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server the ZyXEL Device should use to e-mail logs and alerts. Leave this field blank if you do not want to send logs or alerts by e-mail.
Mail Subject	Enter the subject line used in e-mail messages the ZyXEL Device sends.

Table 61 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Send Log to	Enter the e-mail address to which log entries are sent by e-mail. Leave this field blank if you do not want to send logs by e-mail.
Send Alerts to	Enter the e-mail address to which alerts are sent by e-mail. Leave this field blank if you do not want to send alerts by e-mail.
Log Schedule	Select the frequency with which the ZyXEL Device should send log messages by e-mail. • Daily • Weekly • Hourly • When Log is Full • None. If the **Weekly** or the **Daily** option is selected, specify a time of day when the E-mail should be sent. If the **Weekly** option is selected, then also specify which day of the week the E-mail should be sent. If the **When Log is Full** option is selected, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	This field is only available when you select **Weekly** in the **Log Schedule** field. Select which day of the week to send the logs.
Time for Sending Log	This field is only available when you select **Daily** or **Weekly** in the **Log Schedule** field. Enter the time of day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select this to clear all logs and alert messages after logs are sent by e-mail.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Select this to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that logs the selected categories of logs.
Log Facility	Select a location. The log facility allows you to log the messages in different files in the syslog server. See the documentation of your syslog for more details.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send immediate alert	Select the categories of alerts that you want the ZyXEL Device to send immediately.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

18.3 Log Message Descriptions

The following tables provide descriptions of example log messages.

Table 62 System Error Logs

LOG MESSAGE	DESCRIPTION
WAN connection is down.	The WAN connection is down. You cannot access the network through this interface.
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.

Table 63 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The device has adjusted its time based on information from the time server.
Time calibration failed	The device failed to get information from the time server.
WAN interface gets IP: %s	The WAN interface got a new IP address from the DHCP or PPPoE server.
DHCP client gets %s	A DHCP client got a new IP address from the DHCP server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.
Successful WEB login	Someone has logged on to the device's web configurator interface.
WEB login failed	Someone has failed to log on to the device's web configurator interface.
TELNET Login Successfully	Someone has logged on to the router via telnet.
TELNET Login Fail	Someone has failed to log on to the router via telnet.
Successful FTP login	Someone has logged on to the device via ftp.
FTP login failed	Someone has failed to log on to the device via ftp.
NAT Session Table is Full!	The maximum number of NAT session table entries has been exceeded and the table is full.
Time initialized by Daytime Server	The device got the time and date from the Daytime server.
Time initialized by Time server	The device got the time and date from the time server.
Time initialized by NTP server	The device got the time and date from the NTP server.
Connect to Daytime server fail	The device was not able to connect to the Daytime server.
Connect to Time server fail	The device was not able to connect to the Time server.
Connect to NTP server fail	The device was not able to connect to the NTP server.

Table 63 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
Too large ICMP packet has been dropped	The device dropped an ICMP packet that was too large.
Configuration Change: PC = 0x%x, Task ID = 0x%x	The device is saving configuration changes.

Table 64 Access Control Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: [TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
Firewall rule [NOT] match:[TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>, <rule:%d>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: [TCP | UDP | IGMP | ESP | GRE | OSPF]	The router blocked a packet that didn't have a corresponding NAT table entry.
Router sent blocked web site message: TCP	The router sent a message to notify a user that the router blocked access to a web site that the user requested.
Exceed maximum sessions per host (%d).	The device blocked a session because the host's connections exceeded the maximum sessions per host.
Firewall allowed a packet that matched a NAT session: [TCP | UDP]	A packet from the WAN (TCP or UDP) matched a cone NAT session and the device forwarded it to the LAN.

Table 65 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
Under SYN flood attack, sent TCP RST	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
Exceed TCP MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.)
Peer TCP state out of order, sent TCP RST	The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state.

Table 65 TCP Reset Logs (continued)

LOG MESSAGE	DESCRIPTION
`Firewall session time out, sent TCP RST`	The router sent a TCP reset packet when a dynamic firewall session timed out. The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes TCP reset timeout: 10 seconds
`Exceed MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > "Maximum Incomplete High", the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < "Maximum Incomplete Low".
`Access block, sent TCP RST`	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CI command: `sys firewall tcprst`).

Table 66 Packet Filter Logs

LOG MESSAGE	DESCRIPTION
`[ TCP | UDP | ICMP | IGMP | Generic ] packet filter matched (set: %d, rule: %d)`	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

For type and code details, see Table 74 on page 188.

Table 67 ICMP Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>`	ICMP access matched the default policy and was blocked or forwarded according to the user's setting.
`Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>`	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
`Triangle route packet forwarded: ICMP`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: ICMP`	The router blocked a packet that didn't have a corresponding NAT table entry.

Table 67 ICMP Logs (continued)

LOG MESSAGE	DESCRIPTION
`Unsupported/out-of-order ICMP: ICMP`	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
`Router reply ICMP packet: ICMP`	The router sent an ICMP reply packet to the sender.

Table 68 CDR Logs

LOG MESSAGE	DESCRIPTION
`board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s`	The router received the setup requirements for a call. "call" is the reference (count) number of the call. "dev" is the device type (3 is for dial-up, 6 is for PPPoE). "channel" or "ch" is the call channel ID.For example, "board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 "Means the router has dialed to the PPPoE server 3 times.
`board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s`	The PPPoE or dial-up call is connected.
`board %d line %d channel %d, call %d, %s C02 Call Terminated`	The PPPoE or dial-up call was disconnected.

Table 69 PPP Logs

LOG MESSAGE	DESCRIPTION
`ppp:LCP Starting`	The PPP connection's Link Control Protocol stage has started.
`ppp:LCP Opening`	The PPP connection's Link Control Protocol stage is opening.
`ppp:CHAP Opening`	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
`ppp:IPCP Starting`	The PPP connection's Internet Protocol Control Protocol stage is starting.
`ppp:IPCP Opening`	The PPP connection's Internet Protocol Control Protocol stage is opening.
`ppp:LCP Closing`	The PPP connection's Link Control Protocol stage is closing.
`ppp:IPCP Closing`	The PPP connection's Internet Protocol Control Protocol stage is closing.

Table 70 UPnP Logs

LOG MESSAGE	DESCRIPTION
`UPnP pass through Firewall`	UPnP packets can pass through the firewall.

Table 71 Content Filtering Logs

LOG MESSAGE	DESCRIPTION
%s: Keyword blocking	The content of a requested web page matched a user defined keyword.
%s: Not in trusted web list	The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites.
%s: Forbidden Web site	The web site is in the forbidden web site list.
%s: Contains ActiveX	The web site contains ActiveX.
%s: Contains Java applet	The web site contains a Java applet.
%s: Contains cookie	The web site contains a cookie.
%s: Proxy mode detected	The router detected proxy mode in the packet.
%s: Trusted Web site	The web site is in a trusted domain.
%s	When the content filter is not on according to the time schedule.
Waiting content filter server timeout	The external content filtering server did not respond within the timeout period.
DNS resolving failed	The ZyXEL Device cannot get the IP address of the external content filtering via DNS query.
Creating socket failed	The ZyXEL Device cannot issue a query because TCP/IP socket creation failed, port:port number.
Connecting to content filter server fail	The connection to the external content filtering server failed.
License key is invalid	The external content filtering license key is invalid.

For type and code details, see Table 74 on page 188.

Table 72 Attack Logs

LOG MESSAGE	DESCRIPTION
attack [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack.
land [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack.
ip spoofing - WAN [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected an IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port.
icmp echo : ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack.

Table 72 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
`syn flood TCP`	The firewall detected a TCP syn flood attack.
`ports scan TCP`	The firewall detected a TCP port scan attack.
`teardrop TCP`	The firewall detected a TCP teardrop attack.
`teardrop UDP`	The firewall detected an UDP teardrop attack.
`teardrop ICMP (type:%d, code:%d)`	The firewall detected an ICMP teardrop attack.
`illegal command TCP`	The firewall detected a TCP illegal command attack.
`NetBIOS TCP`	The firewall detected a TCP NetBIOS attack.
`ip spoofing - no routing entry [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall classified a packet with no source routing entry as an IP spoofing attack.
`ip spoofing - no routing entry ICMP (type:%d, code:%d)`	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
`vulnerability ICMP (type:%d, code:%d)`	The firewall detected an ICMP vulnerability attack.
`traceroute ICMP (type:%d, code:%d)`	The firewall detected an ICMP traceroute attack.
ports scan UDP	The firewall detected a UDP port scan attack.
Firewall sent TCP packet in response to DoS attack TCP	The firewall sent TCP packet in response to a DoS attack
ICMP Source Quench ICMP	The firewall detected an ICMP Source Quench attack.
ICMP Time Exceed ICMP	The firewall detected an ICMP Time Exceed attack.
ICMP Destination Unreachable ICMP	The firewall detected an ICMP Destination Unreachable attack.
ping of death. ICMP	The firewall detected an ICMP ping of death attack.
smurf ICMP	The firewall detected an ICMP smurf attack.

Table 73 Remote Management Logs

LOG MESSAGE	DESCRIPTION
Remote Management: FTP denied	Attempted use of FTP service was blocked according to remote management settings.
Remote Management: TELNET denied	Attempted use of TELNET service was blocked according to remote management settings.
Remote Management: HTTP or UPnP denied	Attempted use of HTTP or UPnP service was blocked according to remote management settings.
Remote Management: WWW denied	Attempted use of WWW service was blocked according to remote management settings.
Remote Management: HTTPS denied	Attempted use of HTTPS service was blocked according to remote management settings.

Table 73 Remote Management Logs

LOG MESSAGE	DESCRIPTION
Remote Management: SSH denied	Attempted use of SSH service was blocked according to remote management settings.
Remote Management: ICMP Ping response denied	Attempted use of ICMP service was blocked according to remote management settings.
Remote Management: DNS denied	Attempted use of DNS service was blocked according to remote management settings.

Table 74 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply

Table 74 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 75 SIP Logs

LOG MESSAGE	DESCRIPTION
SIP Registration Success by SIP:SIP Phone Number	The listed SIP account was successfully registered with a SIP register server.
SIP Registration Fail by SIP:SIP Phone Number	An attempt to register the listed SIP account with a SIP register server was not successful.
SIP UnRegistration Success by SIP:SIP Phone Number	The listed SIP account's registration was deleted from the SIP register server.
SIP UnRegistration Fail by SIP:SIP Phone Number	An attempt to delete the listed SIP account's registration from the SIP register server failed.

Table 76 RTP Logs

LOG MESSAGE	DESCRIPTION
Error, RTP init fail	The initialization of an RTP session failed.
Error, Call fail: RTP connect fail	A VoIP phone call failed because the RTP session could not be established.
Error, RTP connection cannot close	The termination of an RTP session failed.

Table 77 FSM Logs: Caller Side

LOG MESSAGE	DESCRIPTION
`VoIP Call Start Ph[Phone Port Number] <- Outgoing Call Number`	Someone used a phone connected to the listed phone port to initiate a VoIP call to the listed destination.
`VoIP Call Established Ph[Phone Port] -> Outgoing Call Number`	Someone used a phone connected to the listed phone port to make a VoIP call to the listed destination.
`VoIP Call End Phone[Phone Port]`	A VoIP phone call made from a phone connected to the listed phone port has terminated.

Table 78 FSM Logs: Callee Side

LOG MESSAGE	DESCRIPTION
`VoIP Call Start from SIP[SIP Port Number]`	A VoIP phone call came to the ZyXEL Device from the listed SIP number.
`VoIP Call Established Ph[Phone Port] <- Outgoing Call Number`	A VoIP phone call was set up from the listed SIP number to the ZyXEL Device.
`VoIP Call End Phone[Phone Port]`	A VoIP phone call that came into the ZyXEL Device has terminated.

Table 79 Lifeline Logs

LOG MESSAGE	DESCRIPTION
`PSTN Call Start`	A PSTN call has been initiated.
`PSTN Call End`	A PSTN call has terminated.
`PSTN Call Established`	A PSTN call has been set up.

CHAPTER 19
Tools

Use these screens to upload new firmware, back up and restore the configuration, and restart the ZyXEL Device.

19.1 Tools Overview

19.1.1 ZyXEL Firmware

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "ZyXEL Device.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Note: Only use firmware for your ZyXEL Device's specific model. Refer to the label on the back of your ZyXEL Device.

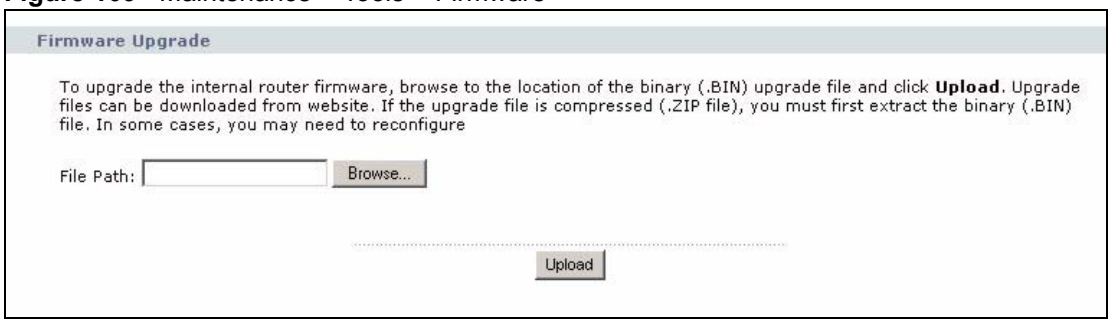
19.2 Tools Screens

19.2.1 Firmware Screen

Use this screen to upload new firmware to the ZyXEL Device. To access this screen, click **Maintenance > Tools > Firmware**.

Note: Only use firmware for your ZyXEL Device's specific model. Refer to the label on the bottom of your ZyXEL Device.

Figure 109 Maintenance > Tools > Firmware


Firmware Upgrade
To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure
File Path:
Browse...
Upload

Each field is described in the following table.

Table 80 Maintenance > Tools > Firmware

LABEL	DESCRIPTION
File Path	Enter the location of the .bin file you want to upload, or click **Browse...** to find it. You must decompress compressed (.zip) files before you can upload them.
Browse...	Click this to find the .bin file you want to upload.
Upload	Click this to begin uploading the selected file. This may take up to two minutes. See Section 19.2.2 on page 192 for more information about this process. **Note:** Do not turn off the device while firmware upload is in progress!

19.2.2 Firmware Upload Screens

Note: Do not turn off the device while firmware upload is in progress!

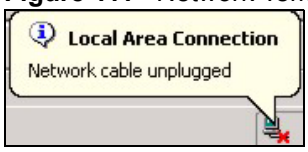
When the ZyXEL Device starts to upload firmware, the **Firmware Upload in Process** screen appears.

Figure 110 Firmware Upload In Process

ZyXEL
Firmware Upload In Process
Please Wait ...
Please wait for the device to finish restarting(SYS LED is on steady). This should take about two minutes. To access the device after a successful firmware upload, you need to log in again. Check your new firmware version in the system status menu.

The process usually takes about two minutes. The device automatically restarts in this time. This causes a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 111 Network Temporarily Disconnected



After two minutes, log in again, and check your new firmware version in the **Status** screen. You might have to open a new browser to log in.

If the upload is not successful, the following screen appears.

Figure 112 Firmware Upload Error

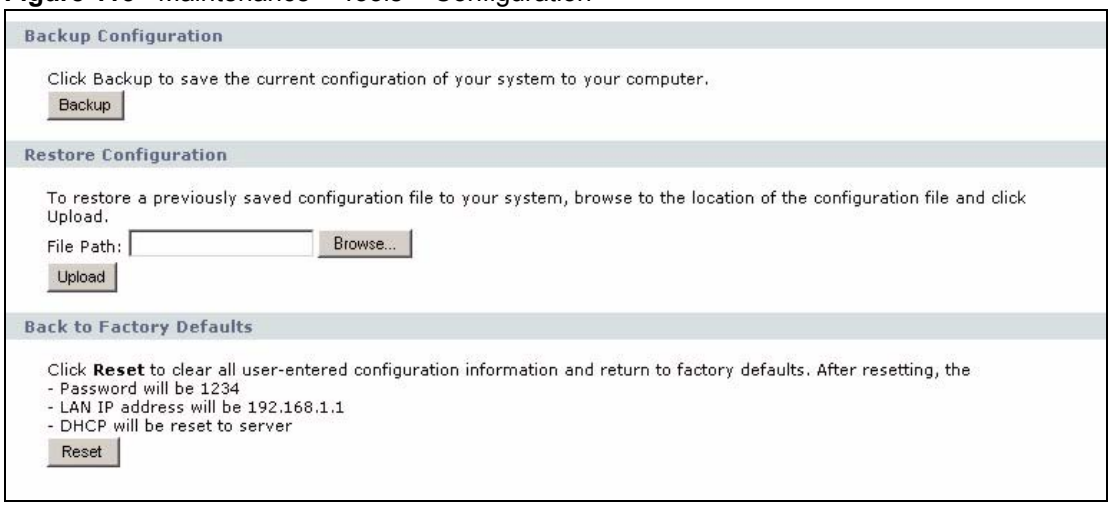
system Upload
Firmware upload error!
The uploaded file was not accepted by the device. Please return to the previous page and select a valid upgrade file. Click Help for more information.
Return

Click **Return** to go back to the **Firmware** screen.

19.2.3 Configuration Screen

Use this screen to back up or restore the configuration of the ZyXEL Device. You can also use this screen to reset the ZyXEL Device to the factory default settings. To access this screen, click **Maintenance > Tools > Configuration**.

Figure 113 Maintenance > Tools > Configuration


Backup Configuration
Click Backup to save the current configuration of your system to your computer.
Backup
Restore Configuration
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.
File Path:
Browse...
Upload
Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server
Reset

Each field is described in the following table.

Table 81 Maintenance > Tools > Configuration

LABEL	DESCRIPTION
Backup Configuration	
Backup	Click this to save the ZyXEL Device's current configuration to a file on your computer. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file is useful if you need to return to your previous settings.
Restore Configuration	
File Path	Enter the location of the file you want to upload, or click **Browse...** to find it.
Browse	Click this to find the file you want to upload.
Upload	Click this to restore the selected configuration file. See Section 19.2.4 on page 194 for more information about this. **Note:** Do not turn off the device while configuration file upload is in progress.
Back to Factory Defaults	
Reset	Click this to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults. There is no warning screen.

19.2.4 Restore Configuration Screens

Note: Do not turn off the device while configuration file upload is in progress.

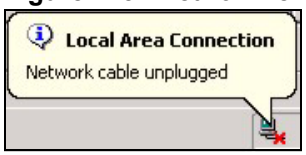
When the ZyXEL Device has finished restoring the selected configuration file, the following screen appears.

Figure 114 Configuration Upload Successful

ZyXEL
Restore Configuration successful
The Device Is Rebooting Now.
After the device finishes rebooting, the login screen displays.

The device now automatically restarts. This causes a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 115 Network Temporarily Disconnected



If the ZyXEL Device's IP address is different in the configuration file you selected, you may need to change the IP address of your computer to be in the same subnet as that of the default management IP address (192.168.5.1). See your Quick Start Guide or the appendices for details on how to set up your computer's IP address.

You might have to open a new browser to log in again.

If the upload was not successful, a **Configuration Upload Error** screen appears.

Figure 116 Configuration Upload Error

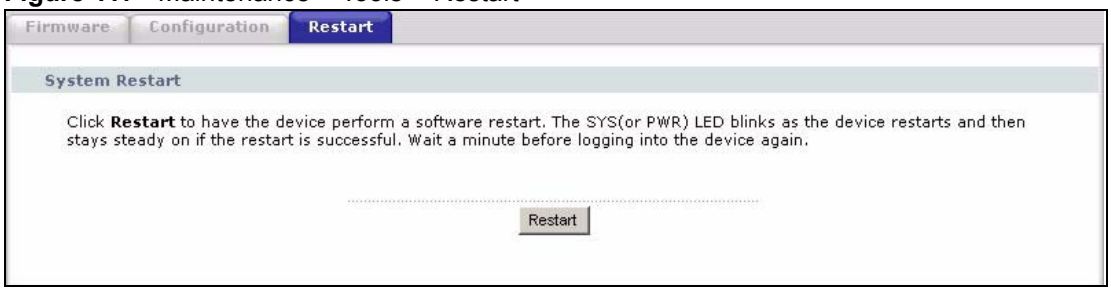
System Restore
Restore configuration error!
The configuration file was not accepted by the device. Please return to the previous page and select a valid configuration file. Click Help for more information.
Return

Click **Return** to go back to the **Configuration** screen.

19.2.5 Restart Screen

Use this screen to reboot the ZyXEL Device without turning the power off. To access this screen, click **Maintenance > Tools > Restart**.

Figure 117 Maintenance > Tools > Restart


Firmware
Configuration
Restart
System Restart
Click Restart to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.
Restart

This does not affect the ZyXEL Device's configuration. When you click **Restart**, the following screen appears.

Figure 118 Maintenance > Tools > Restart > In Progress

ZyXEL
The device is rebooting
The device will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the device again.

Wait one minute for the device to finish restarting. Then, you can log in again.

CHAPTER 20
System

Use this screen to set up general system settings, change the system mode, change the password, configure the DDNS server settings, and set the current date and time.

20.1 System Features Overview

20.1.1 System Name

System Name is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the **Identification** tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings** and **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyXEL Device **System Name**.

20.1.2 Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the ZyXEL Device via DHCP.

20.1.3 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The ZyXEL Device can get the DNS server addresses in the following ways.

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **SYSTEM General** screen.

2 If the ISP did not give you DNS server information, leave the **DNS Server** fields in the **SYSTEM General** screen set to 0.0.0.0 for the ISP to dynamically assign the DNS server IP addresses.

20.1.4 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

Note: If you have a private WAN IP address, then you cannot use Dynamic DNS.

20.1.5 Pre-defined NTP Time Servers List

The ZyXEL Device uses the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Note: The ZyXEL Device can use this pre-defined list of time servers regardless of the Time Protocol you select.

When the ZyXEL Device uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the ZyXEL Device goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

Table 82 Pre-defined NTP Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk

Table 82 Pre-defined NTP Time Servers

ntp1.sp.se
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

20.1.6 Resetting the Time

The ZyXEL Device resets the time in the following instances:

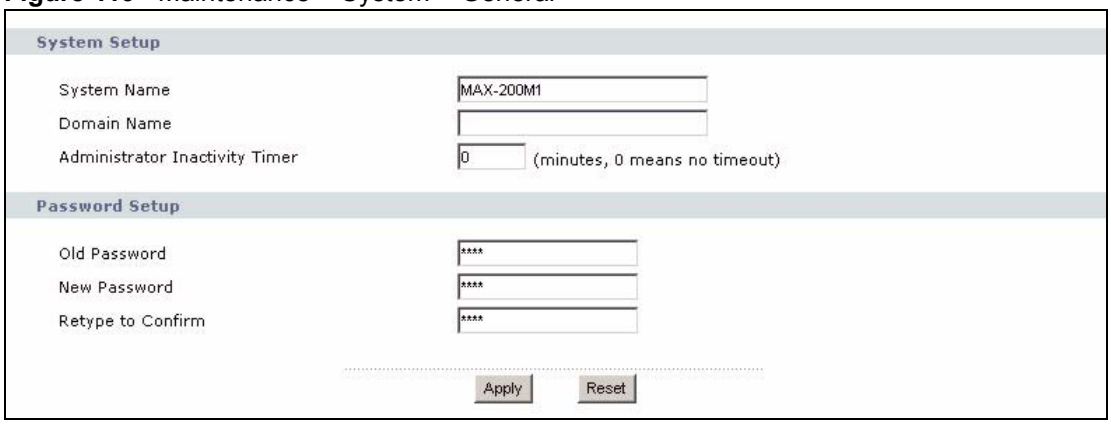
- When the ZyXEL Device starts up.
- When you click **Apply** in the Time Setting Screen.
- 24-hour intervals after starting.

20.2 System Screens

20.2.1 General System Screen

Use this screen to change the ZyXEL Device's mode, set up the ZyXEL Device's system name, domain name, idle timeout, and administrator password. To access this screen, click **Maintenance > System > General**.

Figure 119 Maintenance > System > General



Each field is described in the following table.

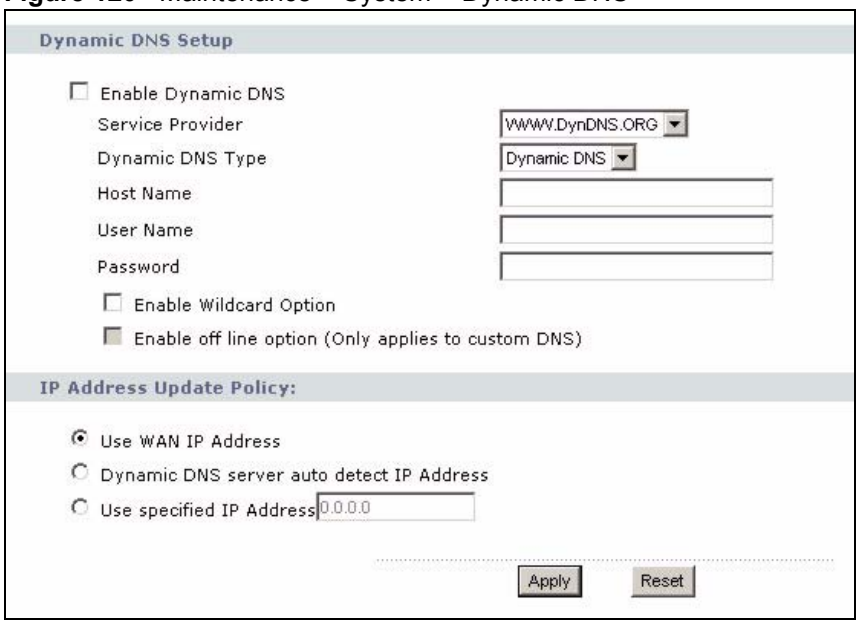
Table 83 Maintenance > System > General

LABEL	DESCRIPTION
System Setup	
System Name	Enter your computer's "Computer Name". This is for identification purposes, but some ISPs also check this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name entry that is propagated to DHCP clients on the LAN. If you leave this blank, the domain name obtained from the ISP is used. Use up to 38 alphanumeric characters. Spaces are not allowed, but dashes "-" and periods "." are accepted.
Administrator Inactivity Timer	Enter the number of minutes a management session can be left idle before the session times out. After it times out, you have to log in again. A value of "0" means a management session never times out, no matter how long it has been left idle. This is not recommended. Long idle timeouts may have security risks. The default is five minutes.
Password Setup	
Old Password	Enter the current password you use to access the ZyXEL Device.
New Password	Enter the new password for the ZyXEL Device. You can use up to 30 characters. As you type the password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Enter the new password again.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its default value.

20.2.2 Dynamic DNS Screen

Use this screen to set up the ZyXEL Device as a dynamic DNS client. To access this screen, click **Maintenance > System > Dynamic DNS**.

Figure 120 Maintenance > System > Dynamic DNS



Each field is described in the following table.

Table 84 Maintenance > System > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Enable Dynamic DNS	Select this to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Enter the host name. You can specify up to two host names, separated by a comma (",").
User Name	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Select this to enable the DynDNS Wildcard feature.
Enable offline option	This field is available when **CustomDNS** is selected in the **DDNS Type** field. Select this if your Dynamic DNS service provider redirects traffic to a URL that you can specify while you are off line. Check with your Dynamic DNS service provider.
IP Address Update Policy	
Use WAN IP Address	Select this if you want the ZyXEL Device to update the domain name with the WAN port's IP address.

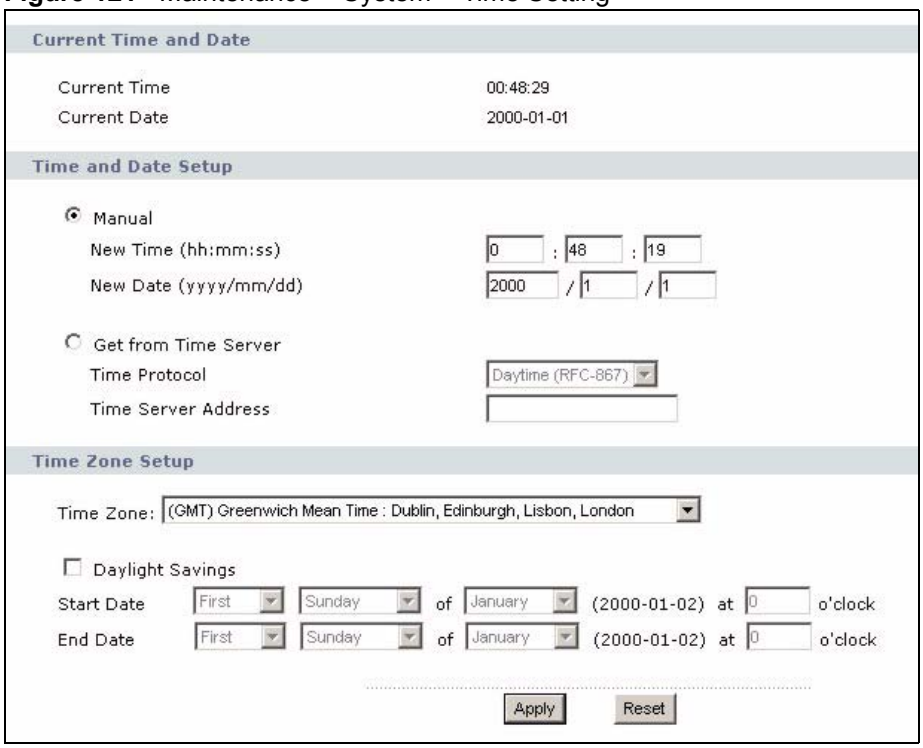
Table 84 Maintenance > System > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS server auto detect IP address	Select this if you want the DDNS server to update the IP address of the host name(s) automatically. Select this option when there are one or more NAT routers between the ZyXEL Device and the DDNS server. **Note:** The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyXEL Device and the DDNS server.
Use specified IP address	Select this if you want to use the specified IP address with the host name(s). Then, specify the IP address. Use this option if you have a static IP address.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its default value.

20.2.3 Time Setting Screen

Use this screen to set the date, time, and time zone in the ZyXEL Device. To access this screen, click **Maintenance > System > Time Setting**.

Figure 121 Maintenance > System > Time Setting



Each field is described in the following table.

Table 85 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time and Date	This section displays the current date and time.
Time and Date Setup	
Manual	Select this if you want to specify the current date and time in the fields below.
New Time	Enter the new time in this field, and click **Apply**.
New Date	Enter the new date in this field, and click **Apply**.
Get from Time Server	Select this if you want to use a time server to update the current date and time in the ZyXEL Device.
Time Protocol	Select the time service protocol that your time server uses.Check with your ISP or network administrator, or use trial-and-error to find a protocol that works. **Daytime (RFC 867)** - This format is day/month/year/time zone. **Time (RFC 868)** - This format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC 1305)** - This format is similar to Time (RFC 868).
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP or network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Select the time zone at your location.

Table 85 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Daylight Savings	Select this if your location uses daylight savings time. Daylight savings is a period from late spring to early fall when many places set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Enter which hour on which day of which week of which month daylight-savings time starts.
End Date	Enter which hour on the which day of which week of which month daylight-savings time ends.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its last-saved value.

CHAPTER 21
Troubleshooting

This chapter covers potential problems and the corresponding remedies.

21.1 Problems Starting Up the ZyXEL Device

Table 86 Troubleshooting Starting Up Your Device

PROBLEM	CORRECTIVE ACTION
None of the lights turn on when I turn on the ZyXEL Device.	Make sure that the ZyXEL Device's power adaptor is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure that the power source is turned on. Remove the power jack, then reinsert it. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

21.2 Problems with the LAN

Table 87 Troubleshooting the LAN

PROBLEM	CORRECTIVE ACTION
The **LAN** light does not turn on.	Check your Ethernet cable connections (refer to the *Quick Start Guide* for details). Check for faulty Ethernet cables.
	Make sure your computer's Ethernet Card is working properly.
I cannot access the ZyXEL Device from the LAN.	If **Any IP** is disabled, make sure that the IP address and the subnet mask of the ZyXEL Device and your computer(s) are on the same subnet.

21.3 Problems with the WAN

Table 88 Troubleshooting the WAN

PROBLEM	CORRECTIVE ACTION
I cannot connect to the Internet.	Check your connection. Look at the **LINK** and **SIGNAL** LEDs on the front of the ZyXEL Device. If the ZyXEL Device cannot detect a signal, follow the steps in Section 21.4 on page 206 to search for a wireless signal. Check your security settings. In the web configurator, go to the **Status** screen. Click **Profile** in the **WiMAX Information** box and make sure that you are using the correct security settings for your Internet account. Check your WiMAX settings. The ZyXEL Device may have been set to search the wrong frequencies for a wireless connection. In the web configurator, go to the **Status** screen. Click **Site Information** in the **WiMAX Information** box and ensure that the values are correct. If the values are incorrect, enter the correct frequency settings in the **Network > WAN > WiMAX Frequency** screen. If you are unsure of the correct values, contact your service provider. Check your IP address settings. You may be using IP address settings incompatible with your Internet account. If you are unsure of the correct settings, contact your service provider. See Appendix C on page 223 for information on how to set up your IP address.
The Internet connection disconnects.	Check your WiMAX link and signal strength using the **LINK** and **SIGNAL** LEDs on the device. See the following section if signal strength is poor or the ZyXEL Device has no link to a base station. Contact your ISP if the problem persists.

21.4 Problems with the Link Quality

Table 89 Troubleshooting Link Quality

PROBLEM	CORRECTIVE ACTION
Internet access is slow or intermittent.	The quality of the ZyXEL Device's wireless connection to the base station may be poor. Poor signal reception may be improved by moving the ZyXEL Device away from thick walls and other obstructions, or to a higher floor in your building. There may be radio interference caused by nearby electrical devices such as microwave ovens and radio transmitters. Move the ZyXEL Device away or switch the other devices off. Weather conditions may also affect signal quality.
	As well as having an external antenna connector, the ZyXEL Device is equipped with an internal directional antenna. If you know the location of the base station, orient the front of the ZyXEL Device (the side with the LEDs) towards the base station. If you do not know the location of the base station, experiment by moving the ZyXEL Device while observing the **SIGNAL** LEDs for an increase in received signal strength.

21.5 Problems Accessing the ZyXEL Device

Table 90 Troubleshooting Accessing Your Device

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyXEL Device.	The default password is "1234". The **Password** field is case-sensitive. Make sure that you enter the correct password, using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.
I cannot access the web configurator.	Make sure that there is not a telnet session running. Use the ZyXEL Device's WAN IP address when configuring from the WAN. Refer to the instructions on checking your WAN connection. Use the ZyXEL Device's LAN IP address when configuring from the LAN. Refer to for instructions on checking your LAN connection. Your computer's and the ZyXEL Device's IP addresses must be on the same subnet for LAN access. If you changed the ZyXEL Device's LAN IP address, then enter the new one as the URL. See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.
	You may also need to clear your Internet browser's cache. In Internet Explorer, click **Tools** and then **Internet Options** to open the **Internet Options** screen. In the **General** tab, click **Delete Files**. In the pop-up window, select the **Delete all offline content** check box and click **OK**. Click **OK** in the **Internet Options** screen to close it. If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address). In Windows, use **arp -d** at the command prompt to delete all entries in your computer's ARP table.
I cannot remotely manage the ZyXEL Device from the LAN or WAN.	Refer to Chapter 21 on page 205 for scenarios when remote management may not be possible.
	Use the ZyXEL Device's WAN IP address when configuring from the WAN. Use the ZyXEL Device's LAN IP address when configuring from the LAN.

21.5.1 Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

21.5.1.1 Internet Explorer Pop-up Blockers

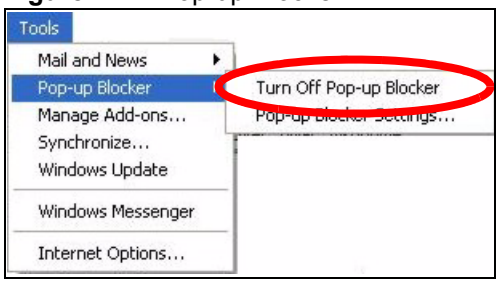
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

21.5.1.1.1 Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 122 Pop-up Blocker

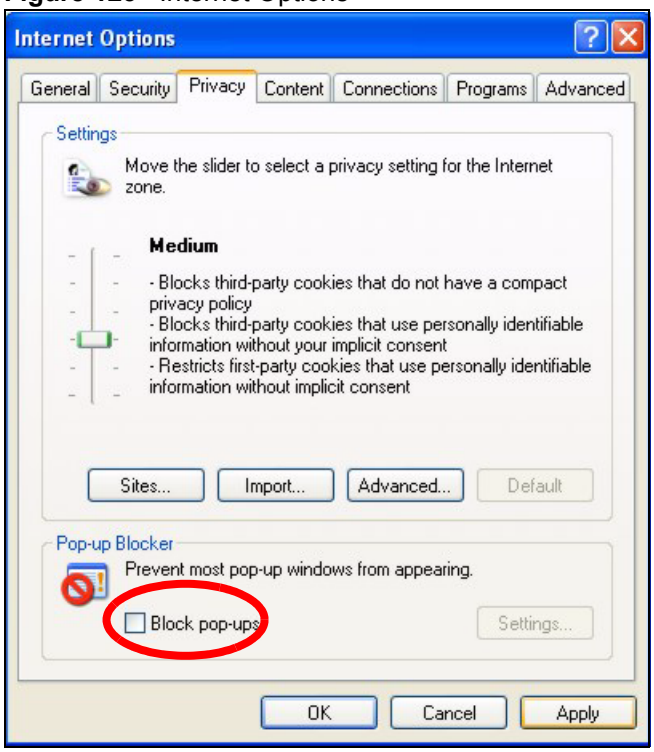


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 123 Internet Options



3 Click **Apply** to save this setting.

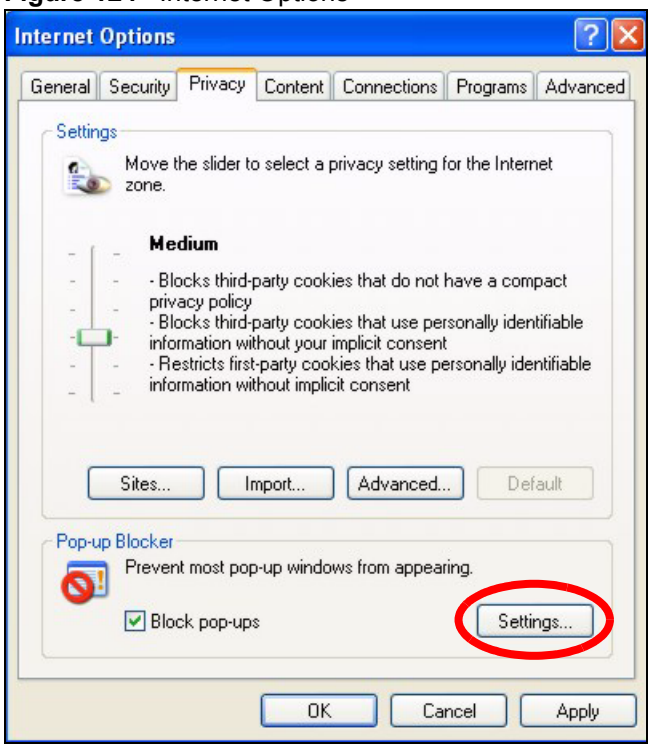
21.5.1.1.2 Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

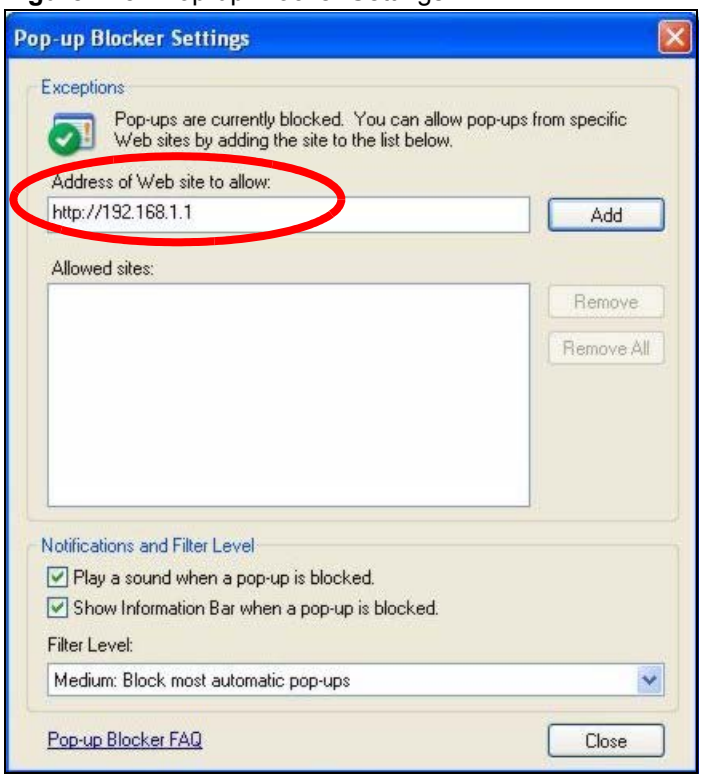
Figure 124 Internet Options



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.1.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 125 Pop-up Blocker Settings


Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.

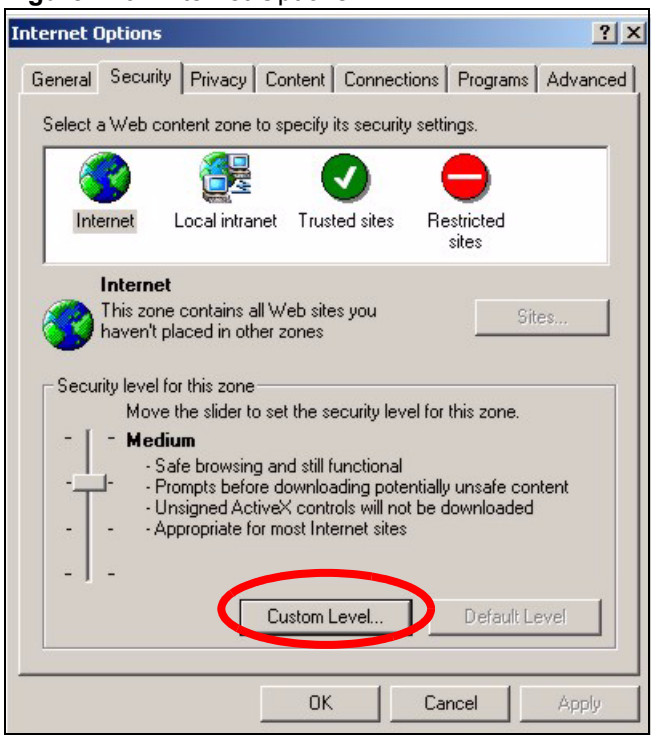
6 Click **Apply** to save this setting.

21.5.1.2 JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 126 Internet Options



2 Click the **Custom Level...** button.

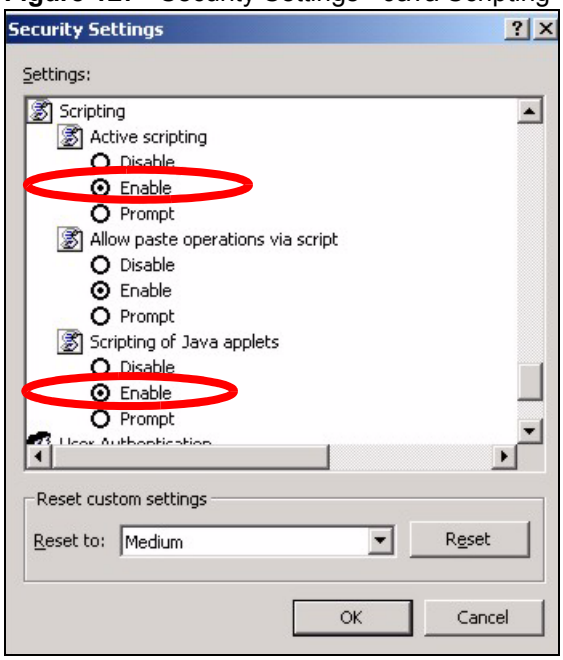
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

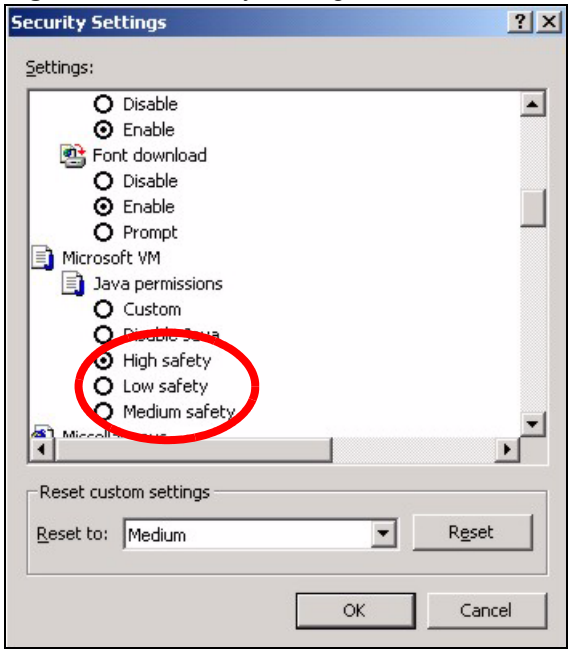
Figure 127 Security Settings - Java Scripting



21.5.1.3 Java Permissions

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2. Click the **Custom Level...** button.
3. Scroll down to **Microsoft VM**.
4. Under **Java permissions** make sure that a safety level is selected.
5. Click **OK** to close the window.

Figure 128 Security Settings - Java



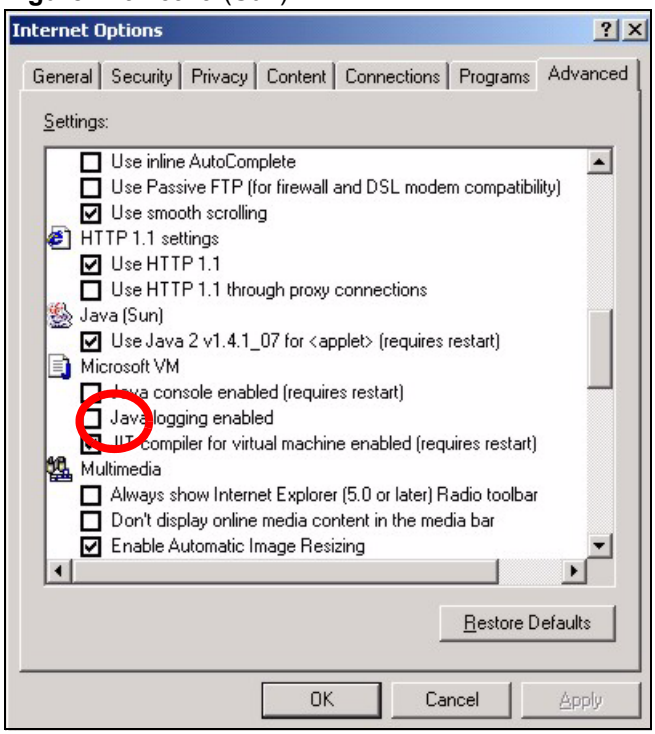
21.5.1.3.1 JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 129 Java (Sun)



21.6 Telephone Problems

Table 91 Troubleshooting Telephone

PROBLEM	CORRECTIVE ACTION
The telephone port won't work or the telephone lacks a dial tone.	Check the telephone connections and telephone wire. Make sure you have the **VoIP SIP Settings** screen properly configured.
I can access the Internet, but cannot make VoIP calls.	Make sure you have the **VoIP SIP Settings** screen properly configured. The **VoIP** LED should come on. Make sure that your telephone is connected to the **LINE** port. You can also check the VoIP status in the **Status** screen. If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you cannot make a call using speed dial, there may be something wrong with the SIP server. Contact your VoIP service provider.

21.7 Problems With Multiple SIP Accounts

You can set up two SIP accounts on your ZyXEL Device. By default your ZyXEL Device uses SIP account 1 for outgoing calls, and it uses SIP accounts 1 and 2 for incoming calls. With this setting, you always use SIP account 1 for your outgoing calls and you cannot distinguish which SIP account the calls are coming in through. If you want to control the use of different dialing plans for accounting purposes or other reasons, you need to configure your phone port in order to control which SIP account you are using when placing or receiving calls.

APPENDIX A
Product Specifications

Table 92 Product Specifications

PHYSICAL AND ENVIRONMENTAL	
Product Name	ZyXEL MAX-200M1 Series IEEE 802.16e Simple Indoor CPE
Interface	Auto-negotiating, auto-MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port
Standards	IEEE 802.16e-2005
Antenna	Built-in patch antenna: 6dBi, 70° azimuth, 30° elevation SMA antenna connector, equipped by default with 2dBi omni antenna, 60°
Operating Temperature	0 ~ 45 degrees Centigrade
Storage Temperature	-25 ~ 55 degrees Centigrade
Operating Humidity	10% ~ 90% (non-condensing)
Storage Humidity	10% ~ 100%
Power Supply	18 V DC
Power consumption	Worst-case-scenario 10W, peak 15W
Weight	389g
Dimensions	120 x 160 x 50mm
RADIO SPECIFICATIONS	
Media Access Protocol	IEEE 802.16e
WiMAX Bandwidth	MAX-200M1: 2.5 - 2.7 GHz MAX-210M1: 3.4 ~ 3.6 GHz MAX-230M1: 2.3 ~ 2.4 GHz
Data Rate	Downlink: Maximum 5 Mbps Uplink: Maximum 2 Mbps
Modulation	QPSK (uplink and downlink) 16-QAM (uplink and downlink) 64-QAM (downlink only)
Output Power	27dBm (+/- 1dB)
Duplex mode	Time Division Duplex (TDD)
SOFTWARE SPECIFICATIONS	
Security	PKMv2 EAP CCMP, 128-bit AES

Table 93 Physical Features

FEATURE	DESCRIPTION
Auto-crossover 10/100 Mbps Ethernet Interface	This interface automatically adjusts to either a crossover or straight-through Ethernet cable.
External Antenna	The ZyXEL Device is equipped with an attached antenna to provide a clear radio connection with the WiMAX base station.
Telephone Port	Connect an analog telephone to the ZyXEL Device's **LINE** port (RJ-11 connector) to take advantage of its Voice over IP (VoIP) features.
Reset Button	The reset button is built into the rear panel. Use this button to restore the factory default password to 1234; IP address to 192.168.1.1, subnet mask to 255.255.255.0 and DHCP server enabled with a pool of 32 IP addresses starting at 192.168.1.33.

Table 94 Non-Physical Features

FEATURE	DESCRIPTION
High Speed Wireless Internet Access	The ZyXEL Device is ideal for high-speed wireless Internet browsing. WiMAX (Worldwide Interoperability for Microwave Access) is a wireless networking standard providing high-bandwidth, wide-range secured wireless service. The ZyXEL Device is a WiMAX mobile station (MS) compatible with the IEEE 802.16e standard.
Firewall	The ZyXEL Device is a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The ZyXEL Device's firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.
Content Filtering	The ZyXEL Device can block access to web sites containing specified keywords. You can define time periods and days during which content filtering is enabled and include or exclude a range of users on the LAN from content filtering.
Any IP	The Any IP feature allows a computer to access the Internet and the ZyXEL Device without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the ZyXEL Device are not in the same subnet.
Auto Provisioning	Your Internet service provider can automatically update your device's configuration via an auto-provisioning server.
Auto Firmware Upgrade	Your device gives you the option to upgrade to a newer firmware version if it finds one during auto-provisioning. Your VoIP service provider must have an auto-provisioning server and a server set up with firmware in order for this feature to work.
Network Address Translation (NAT)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).
Universal Plug and Play (UPnP)	Your device and other UPnP enabled devices can use the standard TCP/IP protocol to dynamically join a network, obtain an IP address and convey their capabilities to each other.

Table 94 Non-Physical Features

FEATURE	DESCRIPTION
Dynamic DNS Support	With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.
DHCP	DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. Your device has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.
Multiple PVC (Permanent Virtual Circuits) Support	Your device supports up to 8 Permanent Virtual Circuits (PVCs).
IP Alias	IP alias allows you to partition a physical network into logical networks over the same Ethernet interface. Your device supports three logical LAN interfaces via its single physical Ethernet interface with the your device itself as the gateway for each LAN network.
IP Policy Routing (IPPR)	Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator.
REN	A Ringer Equivalence Number (REN) is used to determine the number of devices (like telephones or fax machines) that may be connected to the telephone line. Your device has a REN of three, so it can support three devices per telephone port.
Multiple SIP Accounts	You can configure multiple voice (SIP) accounts.
SIP ALG	Your device is a SIP Application Layer Gateway (ALG). It allows VoIP calls to pass through NAT for devices behind it (such as a SIP-based VoIP software application on a computer).
Dynamic Jitter Buffer	The built-in adaptive buffer helps to smooth out the variations in delay (jitter) for voice traffic. This helps ensure good voice quality for your conversations.
Voice Activity Detection/ Silence Suppression	Voice Activity Detection (VAD) reduces the bandwidth that a call uses by not transmitting when you are not speaking.
Comfort Noise Generation	Your device generates background noise to fill moments of silence when the other device in a call stops transmitting because the other party is not speaking (as total silence could easily be mistaken for a lost connection).
Echo Cancellation	You device supports G.168, an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
QoS (Quality of Service)	Quality of Service (QoS) mechanisms help to provide better service on a per-flow basis. Your device supports Type of Service (ToS) tagging. This allows the device to tag voice frames so they can be prioritized over the network.
Packet Filters	Your device's packet filtering function allows added network security and management.

APPENDIX B
WiMAX Security

Wireless security is vital to protect your wireless communications. Without it, information transmitted over the wireless network would be accessible to any networking device within range.

User Authentication and Data Encryption

The WiMAX (IEEE 802.16) standard employs user authentication and encryption to ensure secured communication at all times.

User authentication is the process of confirming a user's identity and level of authorization. Data encryption is the process of encoding information so that it cannot be read by anyone who does not know the code.

WiMAX uses PKMv2 (Privacy Key Management version 2) for authentication, and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Protocol) for data encryption.

WiMAX supports EAP (Extensible Authentication Protocol, RFC 2486) which allows additional authentication methods to be deployed with no changes to the base station or the mobile or subscriber stations.

PKMv2

PKMv2 is a procedure that allows authentication of a mobile or subscriber station and negotiation of a public key to encrypt traffic between the MS/SS and the base station. PKMv2 uses standard EAP methods such as Transport Layer Security (EAP-TLS) or Tunneled TLS (EAP-TTLS) for secure communication.

In cryptography, a 'key' is a piece of information, typically a string of random numbers and letters, that can be used to 'lock' (encrypt) or 'unlock' (decrypt) a message. Public key encryption uses key pairs, which consist of a public (freely available) key and a private (secret) key. The public key is used for encryption and the private key is used for decryption. You can decrypt a message only if you have the private key. Public key certificates (or 'digital IDs') allow users to verify each other's identity.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The base station is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.

- Authorization

  Determines the network services available to authenticated users once they are connected to the network.

- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your base station acts as a message relay between the MS/SS and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the base station and the RADIUS server for user authentication:

- Access-Request

  Sent by an base station requesting authentication.

- Access-Reject

  Sent by a RADIUS server rejecting access.

- Access-Accept

  Sent by a RADIUS server allowing access.

- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The base station sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the base station and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the base station requesting accounting.

- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Diameter

Diameter (RFC 3588) is a type of AAA server that provides several improvements over RADIUS in efficiency, security, and support for roaming.

Security Association

The set of information about user authentication and data encryption between two computers is known as a security association (SA). In a WiMAX network, the process of security association has three stages.

- Authorization request and reply

  The MS/SS presents its public certificate to the base station. The base station verifies the certificate and sends an authentication key (AK) to the MS/SS.

- Key request and reply

  The MS/SS requests a transport encryption key (TEK) which the base station generates and encrypts using the authentication key.

- Encrypted traffic

  The MS/SS decrypts the TEK (using the authentication key). Both stations can now securely encrypt and decrypt the data flow.

CCMP

All traffic in a WiMAX network is encrypted using CCMP (Counter Mode with Cipher Block Chaining Message Authentication Protocol). CCMP is based on the 128-bit Advanced Encryption Standard (AES) algorithm.

'Counter mode' refers to the encryption of each block of plain text with an arbitrary number, known as the counter. This number changes each time a block of plain text is encrypted. Counter mode avoids the security weakness of repeated identical blocks of encrypted text that makes encrypted data vulnerable to pattern-spotting.

'Cipher Block Chaining Message Authentication' (also known as CBC-MAC) ensures message integrity by encrypting each block of plain text in such a way that its encryption is dependent on the block before it. This series of 'chained' blocks creates a message authentication code (MAC or CMAC) that ensures the encrypted data has not been tampered with.

Authentication

The ZyXEL Device supports EAP-TTLS authentication.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection (with EAP-TLS digital certifications are needed by both the server and the wireless clients for mutual authentication). Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

APPENDIX C
Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

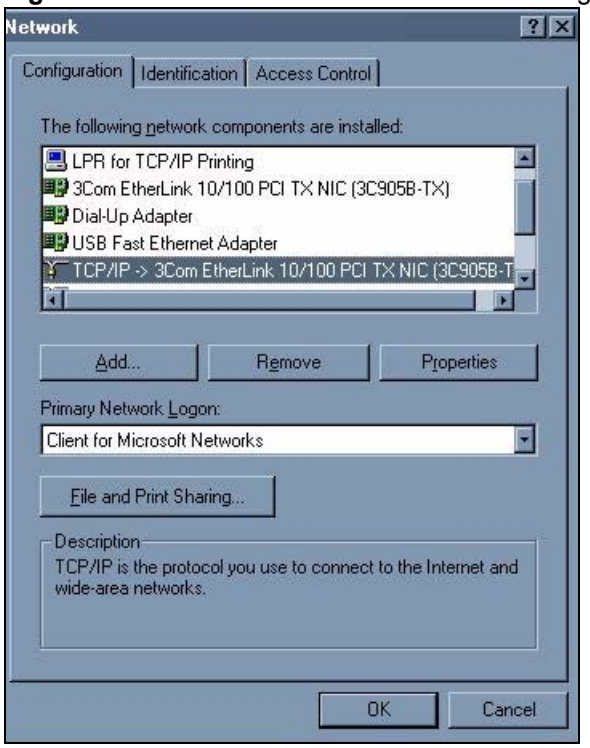
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 130 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

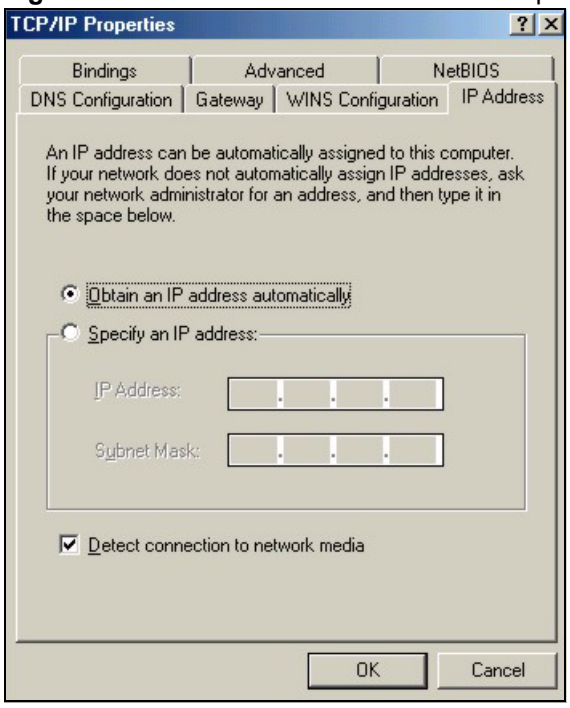
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

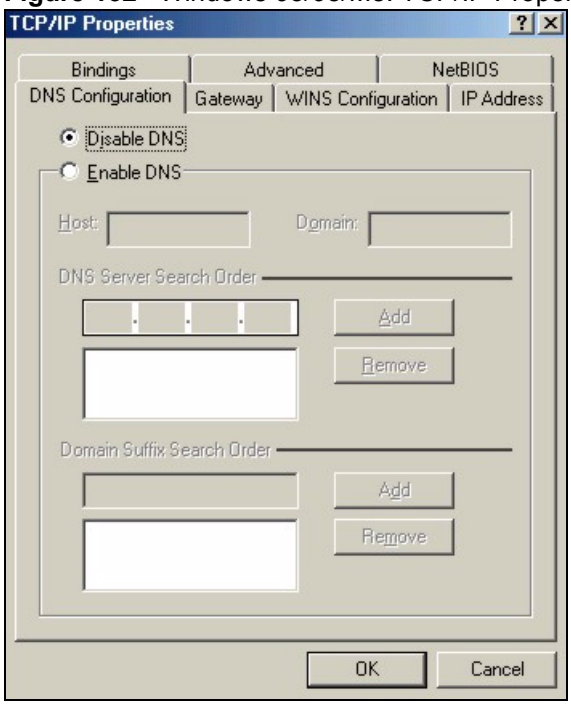
Figure 131 Windows 95/98/Me: TCP/IP Properties: IP Address


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
Detect connection to network media
OK
Cancel

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 132 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

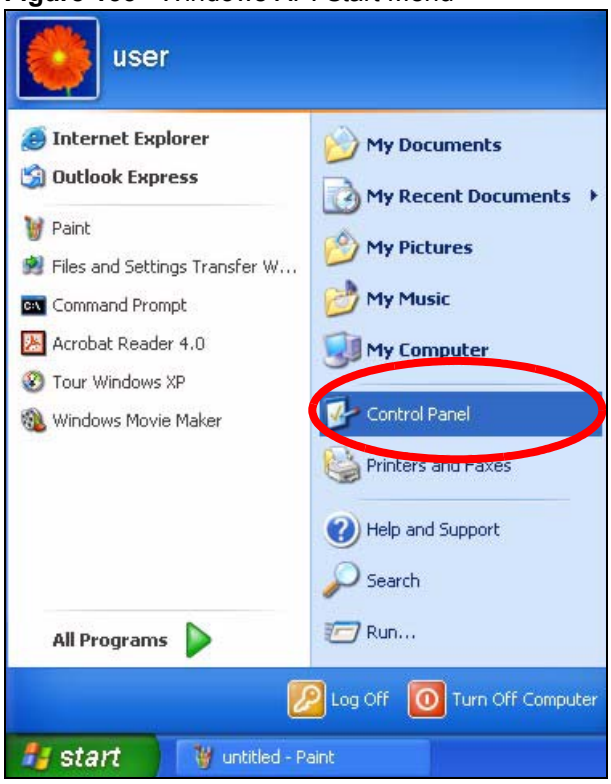
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 133 Windows XP: Start Menu

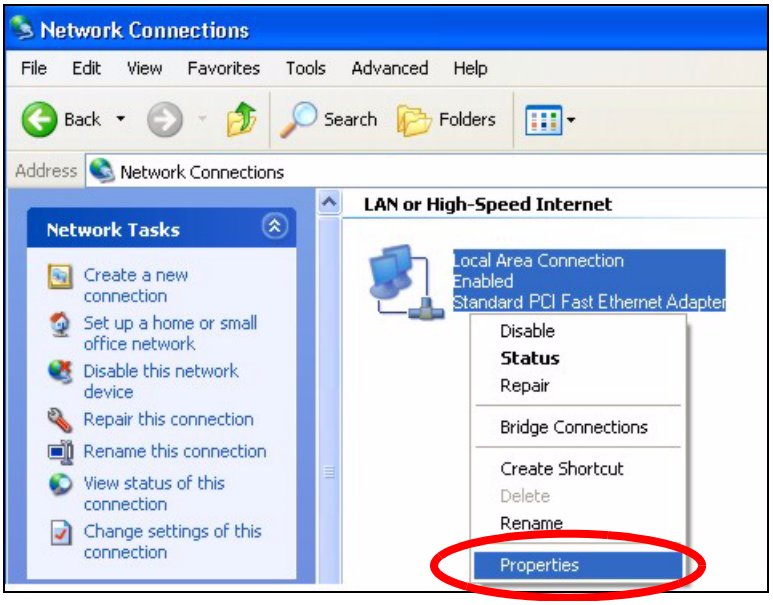


2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 134 Windows XP: Control Panel

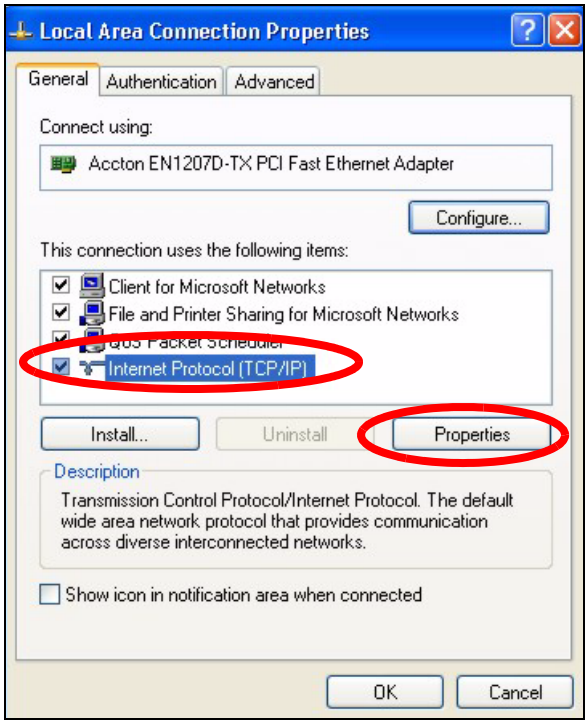
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 135 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Figure 136 Windows XP: Local Area Connection Properties

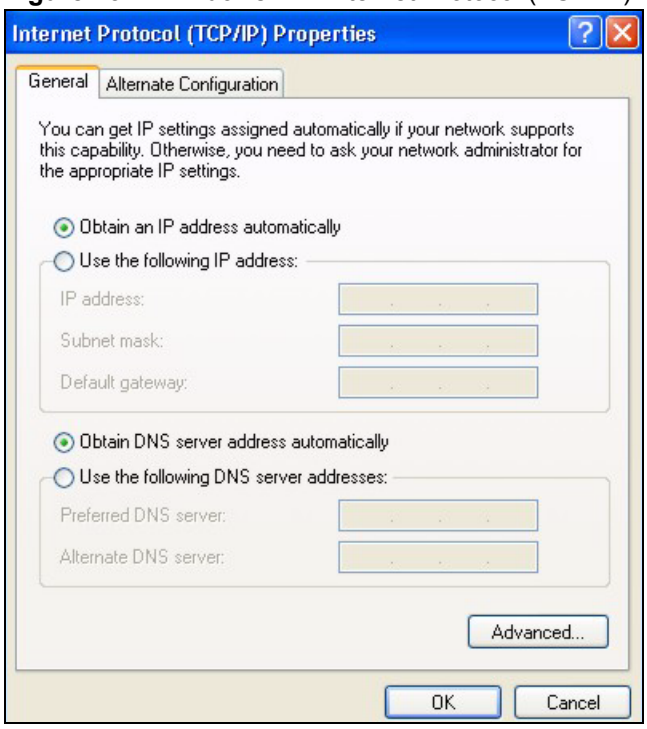

Local Area Connection Properties
General Authentication Advanced
Connect using:
Accton EN1207D-TX PCI Fast Ethernet Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 137 Windows XP: Internet Protocol (TCP/IP) Properties

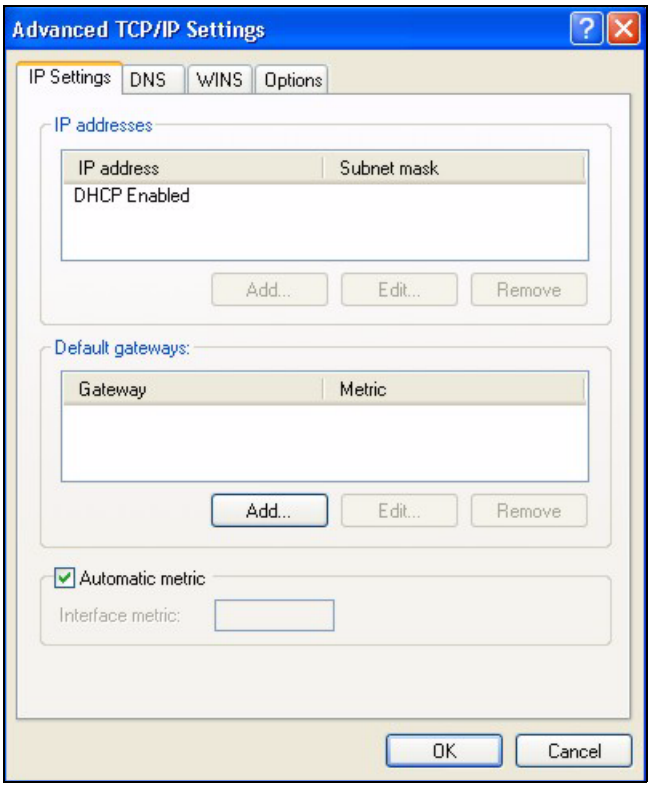

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 138 Windows XP: Advanced TCP/IP Properties

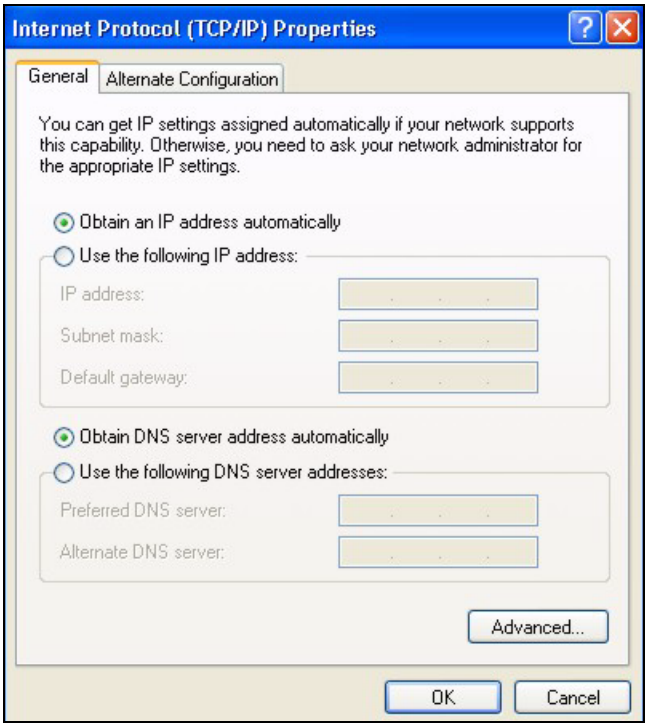


7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 139 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Restart your computer (if prompted).

Verifying Settings

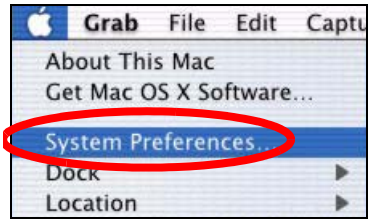
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 140 Macintosh OS X: Apple Menu

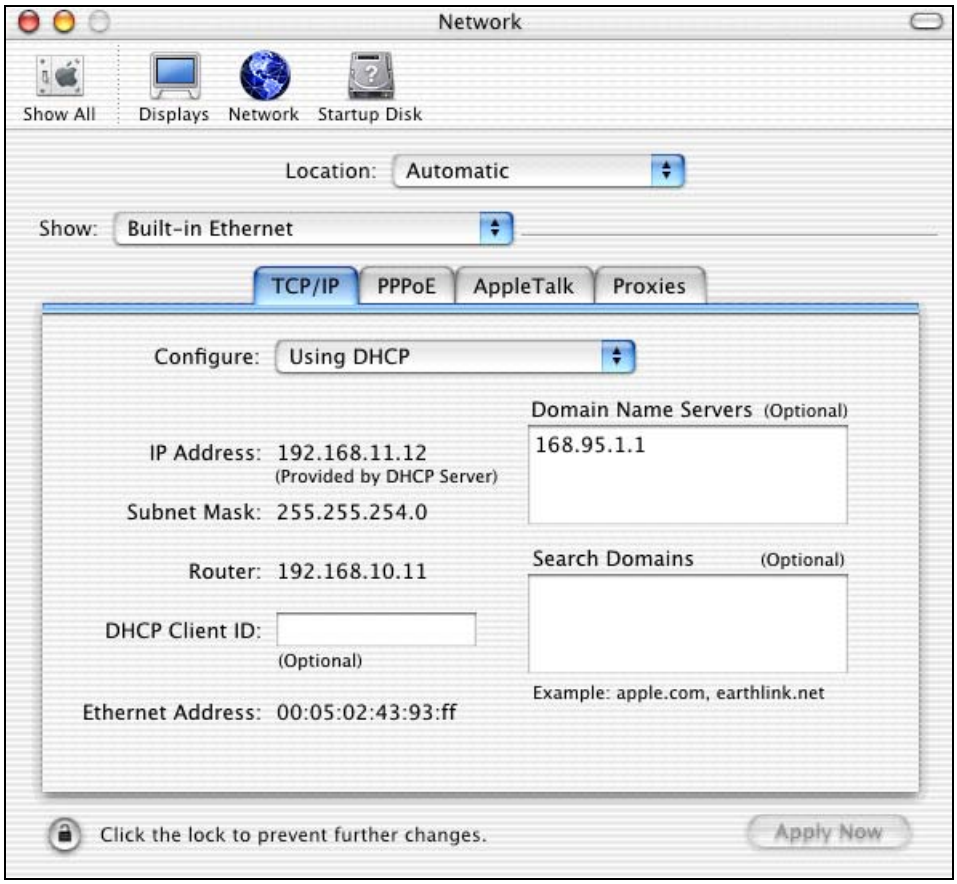


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 141 Macintosh OS X: Network



4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your gateway in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

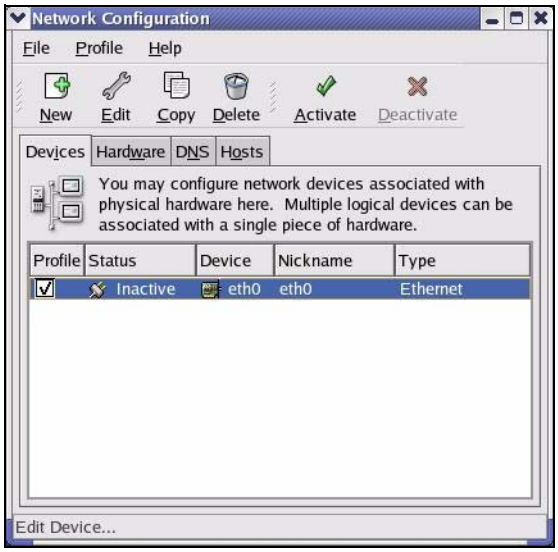
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 142 Red Hat 9.0: KDE: Network Configuration: Devices



2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

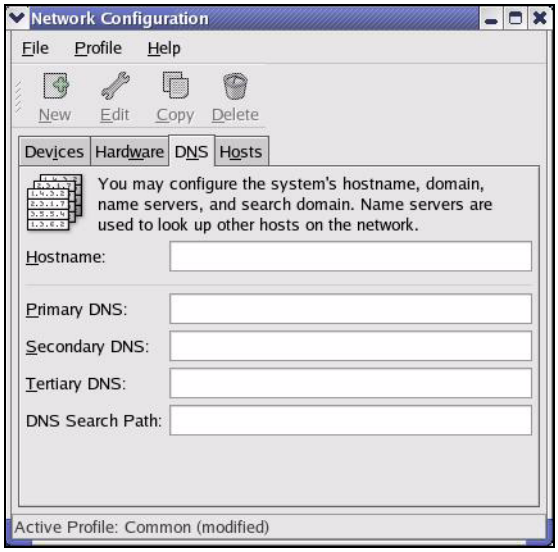
Figure 143 Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 144 Red Hat 9.0: KDE: Network Configuration: DNS



5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes** to save the changes in all screens.

Figure 145 Red Hat 9.0: KDE: Network Configuration: Activate

Question
redhat-config-network:
You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.
Do you want to continue?
No
Yes

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **`dhcp`** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 146 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **`static`** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 147 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 148 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Figure 149 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 150 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129 Bcast:172.23.19.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb) TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

APPENDIX D
IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

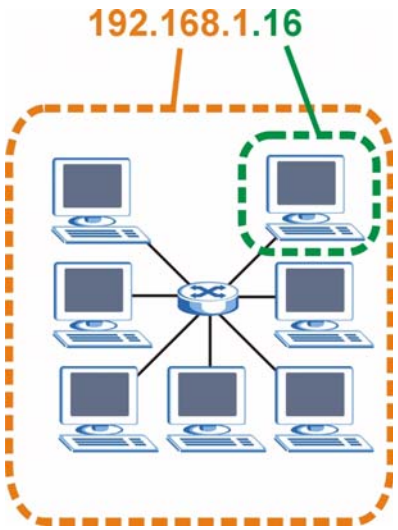
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 151 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 95 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 96 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 97 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 98 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 98 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

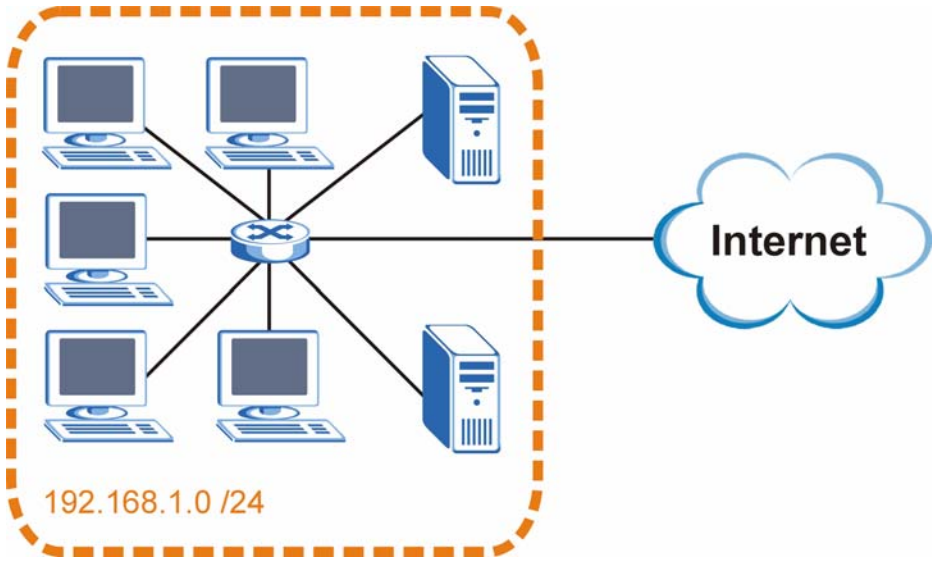
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 152 Subnetting Example: Before Subnetting

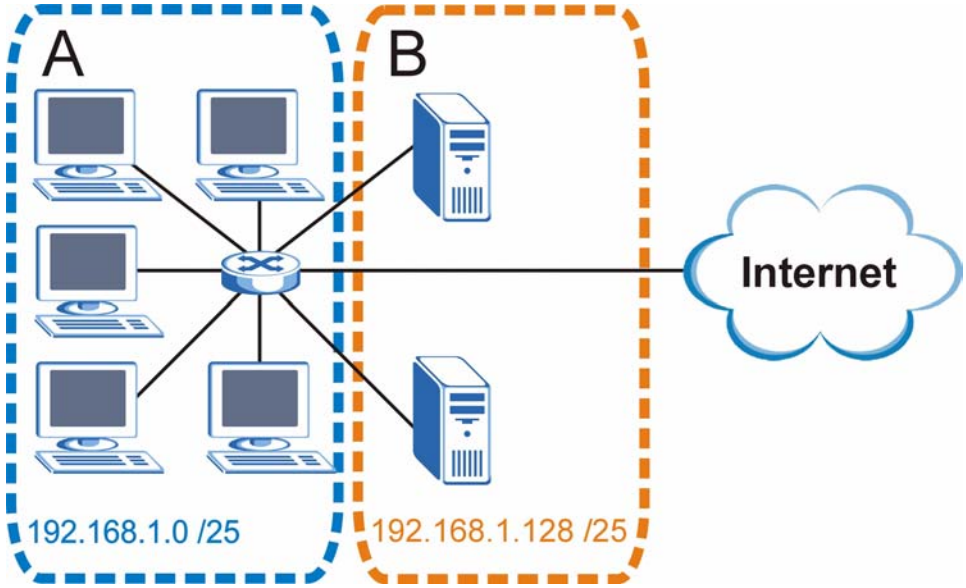


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The "borrowed" host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 153 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 99 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 100 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 101 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 102 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 103 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 103 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 104 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 105 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 105 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ZyXEL Device.

Once you have decided on the network number, pick an IP address for your ZyXEL Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

APPENDIX E
SIP Passthrough

Enabling/Disabling the SIP ALG

You can turn off the ZyXEL Device SIP ALG to avoid retranslating the IP address of an existing SIP device that is using STUN. If you want to use STUN with a SIP client device (a SIP phone or IP phone for example) behind the ZyXEL Device, use the `ip alg disable ALG_SIP` command to turn off the SIP ALG.

Signaling Session Timeout

Most SIP clients have an "expire" mechanism indicating the lifetime of signaling sessions. The SIP UA sends registration packets to the SIP server periodically and keeps the session alive in the ZyXEL Device.

If the SIP client does not have this mechanism and makes no call during the ZyXEL Device SIP timeout default (60 minutes), the ZyXEL Device SIP ALG drops any incoming calls after the timeout period. You can use the `ip alg siptimeout` command to change the timeout value.

Audio Session Timeout

If no voice packets go through the SIP ALG before the timeout period default (5 minutes) expires, the SIP ALG does not drop the call but blocks all voice traffic and deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.

APPENDIX F
Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
    - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
    - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 106 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.

Table 106 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.

Table 106 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

Index

A

AAA 72
about this User's Guide 27
AbS 111
accounting server
  see AAA
ACK message 106
activity 72
address resolution protocol (ARP) 87
advanced encryption standard
  see AES
AES 221
AK 221
ALG 99, 217
alternative subnet mask notation 239
analysis-by-synthesis 111
antenna 215
any IP 216
  note 87
application layer gateway 99, 109, 217
Application Layer Gateway. See ALG.
authentication 65, 72, 73, 219
  inner 222
  types 222
authentication key
  see AK
authentication server
  see AAA
authorization 219
authorization request and reply 221
authorization server
  see AAA
auto firmware upgrade 216
auto-discovering UPnP-enabled network devices 167
automatic log out 35
auto-provisioning 216

B

base station
  see BS
BS 71
  links 71
BYE request 106

C

call hold 122, 124
call service mode 122, 124
call transfer 123, 124
call waiting 123, 124
CBC-MAC 221
CCMP 219, 221
CD 27
cell 71
certificate 219
  verification 221
certifications 4
  notices 5
  viewing 5
chaining 221
chaining message authentication
  see CCMP
change password at login 34
circuit-switched telephone networks 105
Class of Service (CoS) 113
clicks 111
client server
  SIP 106
client-server protocol 106
CMAC
  see MAC
code 219
codec 110
coder/decoder 110
comfort noise 121
comfort noise generation 217
computer IP address 223
computer name 197
configuration 27
configuration upload successful 195
connections 27, 31
contact information 9
copyright 3
CoS 113
counter mode
  see CCMP

coverage area 71
cryptography 219
customer support 9

D

data encryption 219, 221
data flow 221
data rate 215
daytime RFC 867 203
decoder 110
decryption 219, 221
default LAN IP address 33
device name 175
DHCP 197, 198, 217
DHCP client 217
DHCP clients 197
DHCP relay 217
DHCP server 217
DIAMETER 72
differentiated services 113
DiffServ 113
DiffServ Code Point (DSCP) 113
DiffServ code point (DSCP) 113
DiffServ marking rule 113
digital ID 219
dimensions 215
disclaimer 3
DL frequency 78
domain name 197
download frequency
see DL frequency
DS field 113
DSCPs 113
DTMF 111
dual-tone multi-frequency
see DTMF
duplex 215
dynamic DNS 198, 217
dynamic host configuration protocol 217
dynamic jitter buffer 217

E

EAP 72
echo cancellation 121, 217
encoding 219
encrypted traffic 221
encryption 219, 221
environmental specifications 215
ethernet 215
ethernet encapsulation 97
europe type call service mode 122
extensible authorization protocol
see EAP
External Antenna 216

F

FCC interference statement 4
firewall 131, 132
firmware 191
firmware upload 192
firmware upload error 193
flash key 122
flashing 122
frequency band 78
scanning 78
frequency pairs 111
frequency ranges 78
FTP 153, 198
FTP restrictions 153

G

G.168 121, 217
G.711 110
G.729 111
Graphical User Interface (GUI) 29
graphics icons key 28

H

hardware 27, 31
HTTP 191
humidity 215
hybrid waveform codec 111
hypertext transfer protocol 191

I

IANA 244
icons 28
identity 72, 219
idle timeout 154
IEEE 802.16 71, 219
IEEE 802.16e 27, 71
IEEE 802.1Q VLAN 113
IGD 1.0 164
inner authentication 222
install UPnP 164
  Windows Me 164
  Windows XP 166
installation 27, 31
interface 215
interference 206
Internet access 72, 216
Internet access wizard setup 49
Internet Assigned Numbers Authority
  See IANA 244
Internet gateway device 164
Internet service provider
  see ISP
Internet Telephony Service Provider 30
Internet telephony service provider 105
interoperability 71
introduction 29
IP alias 217
IP policy routing (IPPR) 217
IP-PBX 105
ISP 41
ITSP 105
ITU-T 121

J

jitter buffer 217

K

key 65, 73, 219
key request and reply 221

L

language 27
link quality
  troubleshooting 206
listening port 118
log out 35

M

MAC 221
MAN 71
management information base (MIB) 157
manual site survey 78
media access protocol 215
message authentication code
  see MAC
message integrity 221
message waiting indication 111
Metropolitan Area Network
  see MAN
microwave 71
mobile station
  see MS
modulation 215
mouse action sequences 27
MS 71
multimedia 105
multiple PVC support 217
multiple SIP accounts 217
MWI 111

N

NAT 244
  and remote management 154
  server sets 97
NAT routers 109
NAT traversal 163
network activity 72
network address translation (NAT) 216
network address translators 109
network disconnect 193, 195
network services 72
NTP RFC 1305 203
NTP time servers 198

O

OK response 106
operating humidity 215
operating temperature 215
outbound proxy 109, 110
  SIP 110
outbound proxy server 110

P

pattern-spotting 221
PBX services 105
PCM 110
peer-to-peer calls 139
per-hop behavior 113
PHB (per-hop behavior) 113
phone book 139
phone services 121
physical specifications 215
PKMv2 65, 72, 73, 219, 222
plain text encryption 221
port forwarding 97
  port numbers 97
  services 97
port numbers 97
power 215
  output 215
power supply 215
pre-defined NTP time servers list 198
preparation 29
privacy key management
  see PKM
private key 219
product registration 8
product specifications
  see specifications
proxy server
  SIP 107
PSTN 111
public certificate 221
public key 65, 73, 219
Public Switched Telephone Network 111
pulse code modulation 110
pulse dialing 111

Q

QoS 112, 217
quality of service
  see QoS
Quick Start Guide 27, 31, 33

R

radio specifications 215
RADIUS 72, 220
  Shared Secret Key 221
RADIUS Message Types 220
RADIUS Messages 220
real-time transport protocol 108
reception 206
redirect server
  SIP 108
register server
  SIP 108
registration
  product 8
related documentation 27
remote management 153
remote management and NAT 154
remote management limitations 153
REN 217
required bandwidth 111
reset button 35, 194
resetting the time 199
resetting your device 35
RFC 1305 203
RFC 1889 108
RFC 3489 109
RFC 3842 111
RFC 867 203
RFC 868 203
ringer equivalence number 217
RTP 108

S

safety warnings 6
secure communication 65, 73, 219
secure connection 72
security 215, 219

security association 221
see SA
see QoS
see WAN
server, outbound proxy 110
services 72, 97
session initiation protocol
see SIP
silence suppression 121, 217
silent packets 121
SIP 105
ALG 99
authentication 56
authentication password 56
SIP account 105, 217
SIP ACK message 106
SIP ALG 99, 109, 217
SIP application layer gateway 99, 217
SIP BYE request 106
SIP call progression 106
SIP client 106
SIP client server 106
SIP identities 105
SIP INVITE request 106
SIP number 56, 105
SIP OK response 106
SIP outbound proxy 110
SIP proxy server 107
SIP redirect server 108
SIP register server 108
SIP server address 56
SIP servers 106
SIP service domain 56, 106
SIP URI 105
SIP user agent 107
SNMP 156
manager 157
MIBs 157
sound quality 110
specifications 215
physical and environmental 215
radio 215
speed dial 139
SS 71
standards 215
stateful inspection 131
storage humidity 215
storage temperature 215
STUN 109
subnet 237
subnet mask 238
subnetting 240
subscriber station
see SS
supplementary phone services 121
support 27
support CD 27
syntax conventions 27
system name 197
system timeout 154

T

tampering
TDD 215
TEK 221
telephone keys 111
temperature 215
terms 27
TFTP restrictions 153
three-way conference 123, 125
time
resetting 199
time RFC 868 203
TLS 65, 73, 219
ToS 112
Touch Tone® 111
trademarks 3
transport encryption key
see TEK
transport layer security
see TLS
triangle 134
triangle route
solutions 134
trigger port forwarding 98
process 98
troubleshooting
link quality 206
TTLS 65, 73, 219, 222
tunneled TLS
see TTLS
Type of Service 112

U

UIC 164
unauthorized device 219

uniform resource identifier **105**
Universal Plug and Play **163**
  application **163**
  security issues **163**
Universal Plug and Play (UPnP) **216**
Universal Plug and Play Forum **164**
UPnP **163**, **175**
  auto-discovery **167**
  installing example **164**
UPnP certification **164**
USA type call service mode **124**
use NAT **109**
user agent, SIP **107**
user authentication **219**
user ID **56**
user name **201**

V

VAD **121**, **217**
verification **221**
virtual local area network
  see VLAN
VLAN **113**
VLAN group **113**
VLAN ID **113**
VLAN ID tags **113**
VLAN tags **113**
voice activity detection **121**, **217**
voice coding **110**
voice mail **105**
voice over IP
  see VoIP
VoIP **27**, **105**
  standards compliance **217**

W

WAN **71**
WAN setup **71**
warranty **8**
  note **8**
waveform codec **110**
weather conditions **206**
web configurator **33**
weight **215**
wide area network
WiMAX **27**, **71**, **215**
  security **221**
  WiMAX Forum **71**
WiMAX bandwidth **215**
Wireless Interoperability for Microwave Access
  see WiMAX
wireless Metropolitan Area Network
  see MAN
wireless network **27**
  access **71**
  standard **71**
wireless security **215**, **219**
wizard setup **49**

Z

ZyXEL utility **29**, **31**